Monday, October 25
2:30pm-4:00pm

304 - International Privacy Issues

William Calore
Director of Contracts
RTI International

Bill Cosden
General Counsel
Silver Oak Partners

Renard Francois
Legal Services Division
Catepillar

Session 304

Faculty Biographies

William Calore

William J. Calore is the director of contracts for the RTI International, a world-renown non-profit research institute located in Research Triangle Park, NC. His responsibilities include supporting the Advanced Technology and Energy Group, drafting and negotiating agreements, and providing advice and counsel regarding international and intellectual property matters.

Prior to joining RTI International, Mr. Calore worked for several multi-national companies, including Volvo, Atlas Copco, Reichhold, in a variety of capacities, including assistant general counsel and general counsel, and most recently, SRA International, where he served as director of corporate legal compliance. During his career, he has lived in Europe on two separate occasions, and has worked on numerous international strategic relationships, joint ventures, M&A, and international/cross-border transactions. Mr. Calore has extensive experience handling international employment and compliance related matters in Europe, the Middle East, Africa, Asia, SE Asia, and South America, as well as being an experienced government contracting lawyer.

Mr. Calore has spoken at numerous conferences both in the USA and China.

He received his BA from Holy Cross College in Worcester, MA, and is a graduate of the Washington & Lee University School of Law.

Bill Cosden

Bill Cosden is general counsel of Silver Oak Partners, a financial services company, focusing in the software technology sector.

Previously, Mr. Cosden served as director of legal affairs, for Beyond.com, an e-commerce services provider, where he provided and managed legal services for e-commerce stores operating in six continents. Before joining Beyond.com, he was corporate counsel for ten years with the Pacific, Gas & Electric Company ("PG&E"), where his responsibilities included antitrust, commercial, environmental and tort litigation, unlawful business practices defense, and internal investigations and regulatory compliance. Prior to PG&E, he was a senior deputy district attorney with the Alameda County (CA) district attorney's office. Responsibilities there included civil and criminal white-collar crime, environmental enforcement, and prosecution of unlawful business practices.

Mr. Cosden is a past President of ACC's San Francisco Bay Area Chapter, and is co-founder of the annual Stanford Ecommerce Best Practices Conference, now in its seventh year.

He received a BS from the University of California, Berkeley and received his JD from the University of San Francisco, School of Law.

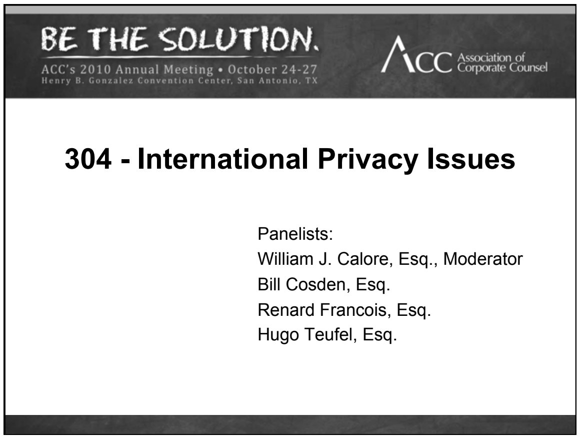
Renard Francois

Renard Francois is the privacy counsel for Caterpillar Inc. in Peoria, Illinois. His responsibilities include working with business units to comply with applicable privacy and data security laws and regulations.

Prior to joining Caterpillar, Mr. Francois was an associate attorney at Bass, Berry & Sims in Nashville, Tennessee, where he worked in the litigation and intellectual property departments. Before joining the firm, Mr. Francois was an attorney at the Federal Trade Commission where he focused on privacy issues.

Currently, he serves on the Department of Homeland Security's Data Privacy & Integrity Advisory Committee and is a member of the Advisory Board of the Center of Privacy and Information Technology.

Mr. Francois received his BA from the University of Pennsylvania, his JD from the George Washington Law School, and an LLM from the John Marshall Law School in Chicago.



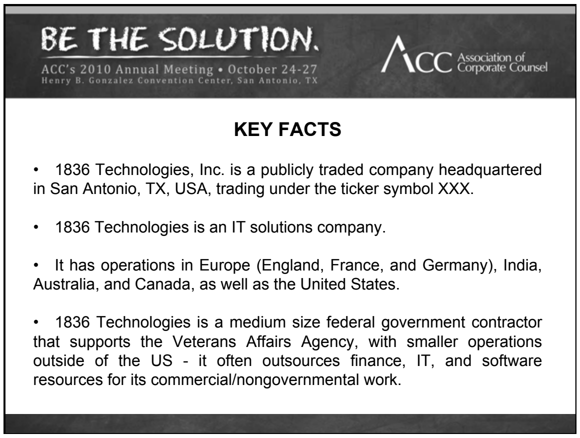
BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

304 - International Privacy Issues

Panelists:
William J. Calore, Esq., Moderator
Bill Cosden, Esq.
Renard Francois, Esq.
Hugo Teufel, Esq.



BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

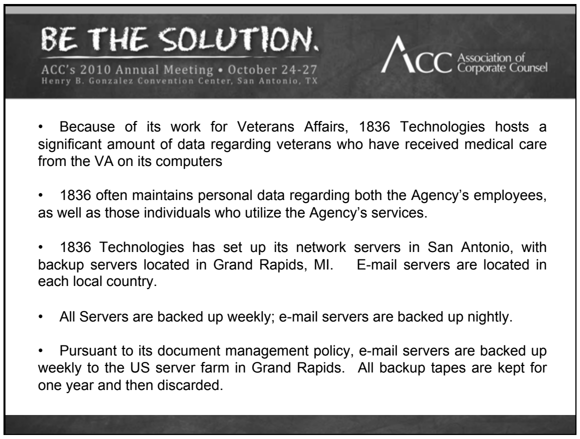
KEY FACTS

- 1836 Technologies, Inc. is a publicly traded company headquartered in San Antonio, TX, USA, trading under the ticker symbol XXX.

- 1836 Technologies is an IT solutions company.

- It has operations in Europe (England, France, and Germany), India, Australia, and Canada, as well as the United States.

- 1836 Technologies is a medium size federal government contractor that supports the Veterans Affairs Agency, with smaller operations outside of the US - it often outsources finance, IT, and software resources for its commercial/nongovernmental work.



BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

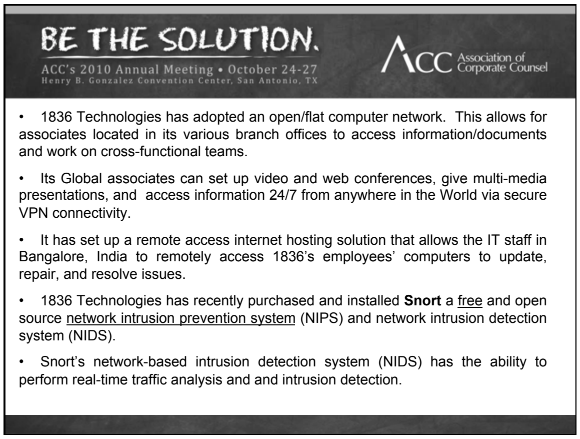
- Because of its work for Veterans Affairs, 1836 Technologies hosts a significant amount of data regarding veterans who have received medical care from the VA on its computers

- 1836 often maintains personal data regarding both the Agency's employees, as well as those individuals who utilize the Agency's services.

- 1836 Technologies has set up its network servers in San Antonio, with backup servers located in Grand Rapids, MI. E-mail servers are located in each local country.

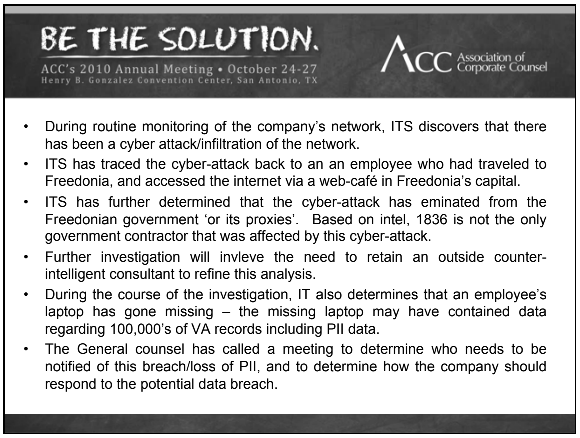
- All Servers are backed up weekly; e-mail servers are backed up nightly.

- Pursuant to its document management policy, e-mail servers are backed up weekly to the US server farm in Grand Rapids. All backup tapes are kept for one year and then discarded.



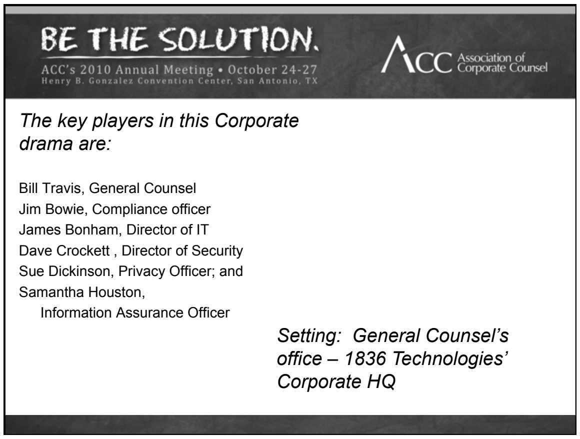
BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

- 1836 Technologies has adopted an open/flat computer network. This allows for associates located in its various branch offices to access information/documents and work on cross-functional teams.
- Its Global associates can set up video and web conferences, give multi-media presentations, and access information 24/7 from anywhere in the World via secure VPN connectivity.
- It has set up a remote access internet hosting solution that allows the IT staff in Bangalore, India to remotely access 1836's employees' computers to update, repair, and resolve issues.
- 1836 Technologies has recently purchased and installed **Snort** a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS).
- Snort's network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and and intrusion detection.



BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

- During routine monitoring of the company's network, ITS discovers that there has been a cyber attack/infiltration of the network.
- ITS has traced the cyber-attack back to an an employee who had traveled to Freedonia, and accessed the internet via a web-café in Freedonia's capital.
- ITS has further determined that the cyber-attack has eminated from the Freedonian government 'or its proxies'. Based on intel, 1836 is not the only government contractor that was affected by this cyber-attack.
- Further investigation will invleve the need to retain an outside counter-intelligent consultant to refine this analysis.
- During the course of the investigation, IT also determines that an employee's laptop has gone missing – the missing laptop may have contained data regarding 100,000's of VA records including PII data.
- The General counsel has called a meeting to determine who needs to be notified of this breach/loss of PII, and to determine how the company should respond to the potential data breach.

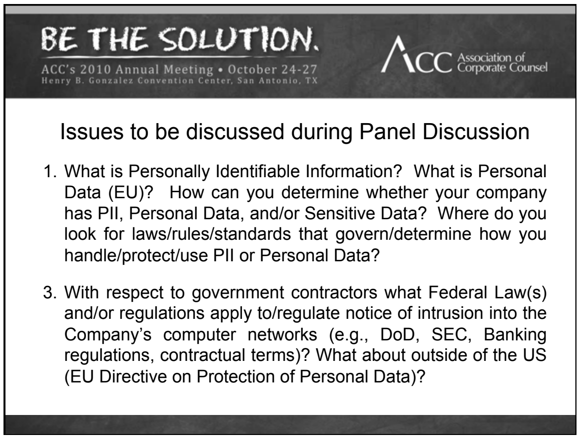


BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

The key players in this Corporate drama are:

Bill Travis, General Counsel
Jim Bowie, Compliance officer
James Bonham, Director of IT
Dave Crockett , Director of Security
Sue Dickinson, Privacy Officer; and
Samantha Houston,
Information Assurance Officer

Setting: General Counsel's office – 1836 Technologies' Corporate HQ



BE THE SOLUTION.

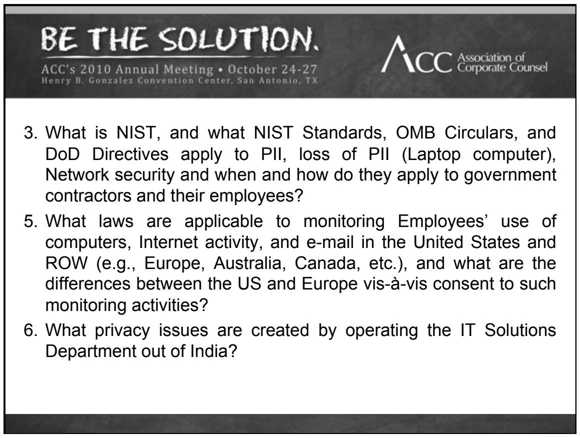
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

Issues to be discussed during Panel Discussion

1. What is Personally Identifiable Information? What is Personal Data (EU)? How can you determine whether your company has PII, Personal Data, and/or Sensitive Data? Where do you look for laws/rules/standards that govern/determine how you handle/protect/use PII or Personal Data?

3. With respect to government contractors what Federal Law(s) and/or regulations apply to/regulate notice of intrusion into the Company's computer networks (e.g., DoD, SEC, Banking regulations, contractual terms)? What about outside of the US (EU Directive on Protection of Personal Data)?

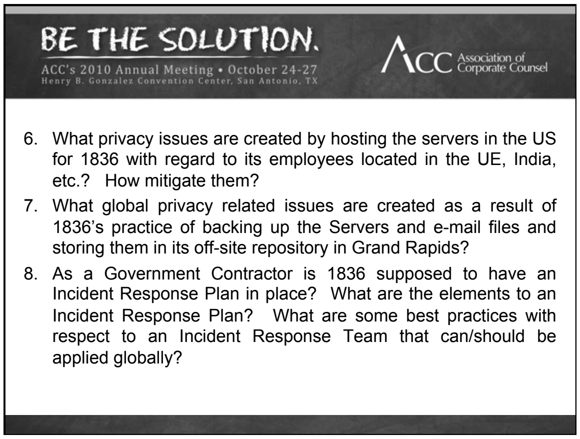


BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

3. What is NIST, and what NIST Standards, OMB Circulars, and DoD Directives apply to PII, loss of PII (Laptop computer), Network security and when and how do they apply to government contractors and their employees?
5. What laws are applicable to monitoring Employees' use of computers, Internet activity, and e-mail in the United States and ROW (e.g., Europe, Australia, Canada, etc.), and what are the differences between the US and Europe vis-à-vis consent to such monitoring activities?
6. What privacy issues are created by operating the IT Solutions Department out of India?

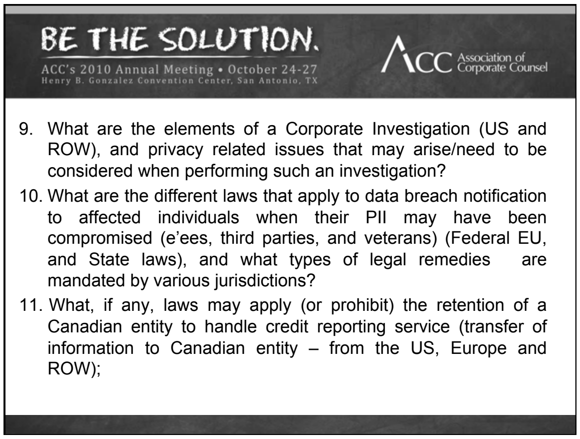


BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

6. What privacy issues are created by hosting the servers in the US for 1836 with regard to its employees located in the UE, India, etc.? How mitigate them?
7. What global privacy related issues are created as a result of 1836's practice of backing up the Servers and e-mail files and storing them in its off-site repository in Grand Rapids?
8. As a Government Contractor is 1836 supposed to have an Incident Response Plan in place? What are the elements to an Incident Response Plan? What are some best practices with respect to an Incident Response Team that can/should be applied globally?

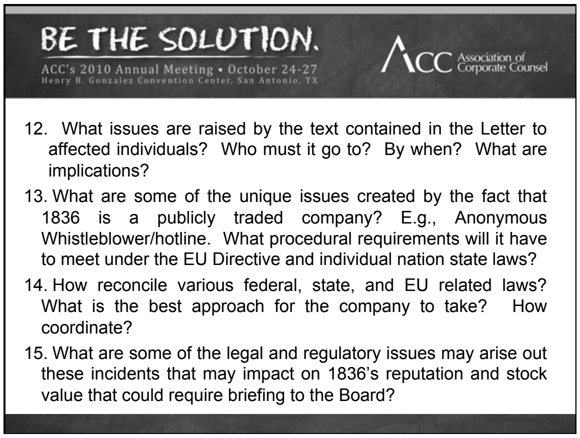


BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

9. What are the elements of a Corporate Investigation (US and ROW), and privacy related issues that may arise/need to be considered when performing such an investigation?
10. What are the different laws that apply to data breach notification to affected individuals when their PII may have been compromised (e'ees, third parties, and veterans) (Federal EU, and State laws), and what types of legal remedies are mandated by various jurisdictions?
11. What, if any, laws may apply (or prohibit) the retention of a Canadian entity to handle credit reporting service (transfer of information to Canadian entity – from the US, Europe and ROW);

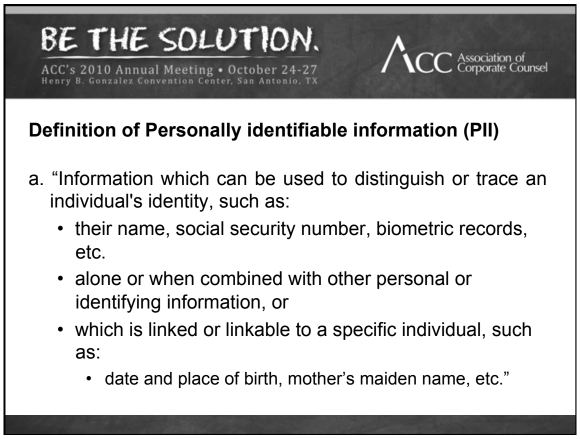


BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

12. What issues are raised by the text contained in the Letter to affected individuals? Who must it go to? By when? What are implications?
13. What are some of the unique issues created by the fact that 1836 is a publicly traded company? E.g., Anonymous Whistleblower/hotline. What procedural requirements will it have to meet under the EU Directive and individual nation state laws?
14. How reconcile various federal, state, and EU related laws? What is the best approach for the company to take? How coordinate?
15. What are some of the legal and regulatory issues may arise out these incidents that may impact on 1836's reputation and stock value that could require briefing to the Board?



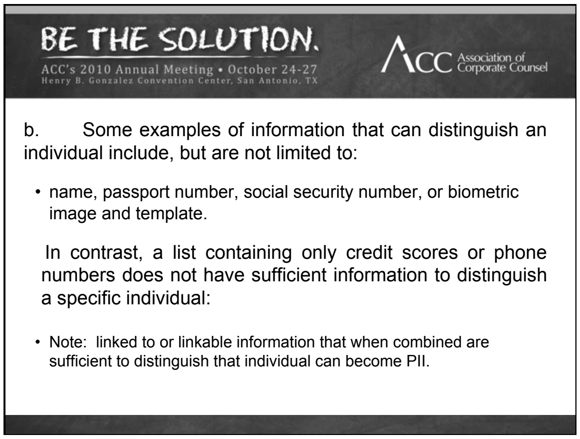
BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

Definition of Personally identifiable information (PII)

a. "Information which can be used to distinguish or trace an individual's identity, such as:
   - their name, social security number, biometric records, etc.
   - alone or when combined with other personal or identifying information, or
   - which is linked or linkable to a specific individual, such as:
     - date and place of birth, mother's maiden name, etc."

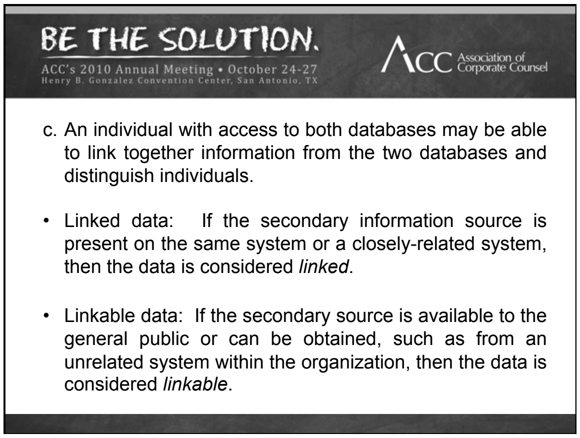

BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

b. Some examples of information that can distinguish an individual include, but are not limited to:

- name, passport number, social security number, or biometric image and template.

In contrast, a list containing only credit scores or phone numbers does not have sufficient information to distinguish a specific individual:

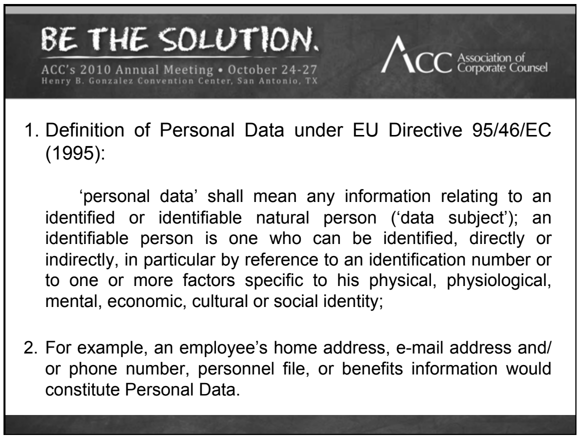
- Note: linked to or linkable information that when combined are sufficient to distinguish that individual can become PII.


BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

c. An individual with access to both databases may be able to link together information from the two databases and distinguish individuals.

- Linked data: If the secondary information source is present on the same system or a closely-related system, then the data is considered *linked*.

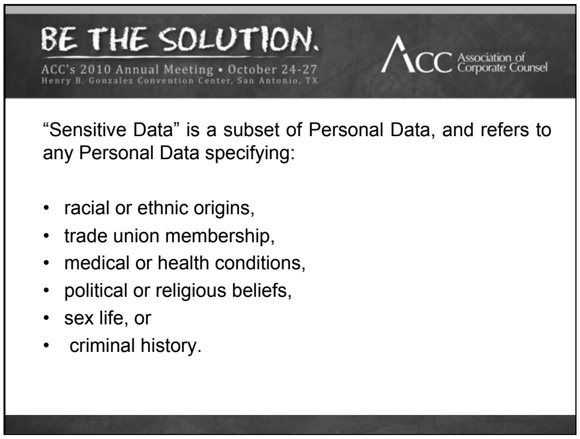
- Linkable data: If the secondary source is available to the general public or can be obtained, such as from an unrelated system within the organization, then the data is considered *linkable*.


BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX
ACC Association of Corporate Counsel

1. Definition of Personal Data under EU Directive 95/46/EC (1995):

   'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

2. For example, an employee's home address, e-mail address and/or phone number, personnel file, or benefits information would constitute Personal Data.



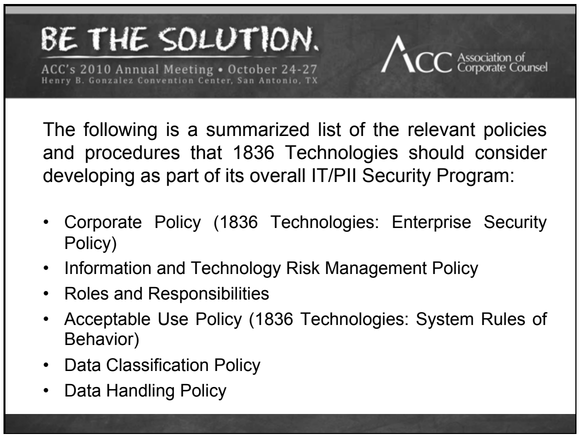
BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

"Sensitive Data" is a subset of Personal Data, and refers to any Personal Data specifying:

- racial or ethnic origins,
- trade union membership,
- medical or health conditions,
- political or religious beliefs,
- sex life, or
- criminal history.



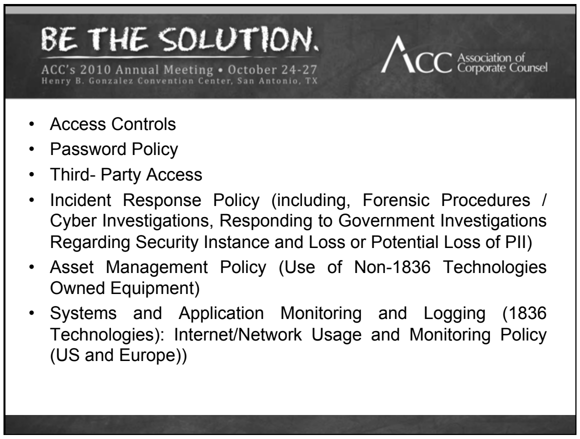
BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

The following is a summarized list of the relevant policies and procedures that 1836 Technologies should consider developing as part of its overall IT/PII Security Program:

- Corporate Policy (1836 Technologies: Enterprise Security Policy)
- Information and Technology Risk Management Policy
- Roles and Responsibilities
- Acceptable Use Policy (1836 Technologies: System Rules of Behavior)
- Data Classification Policy
- Data Handling Policy

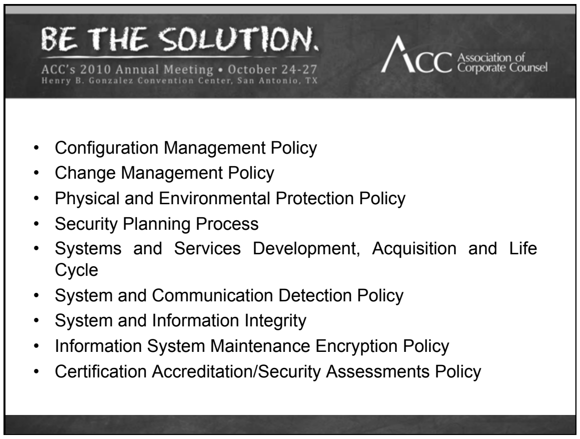


BE THE SOLUTION.

ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

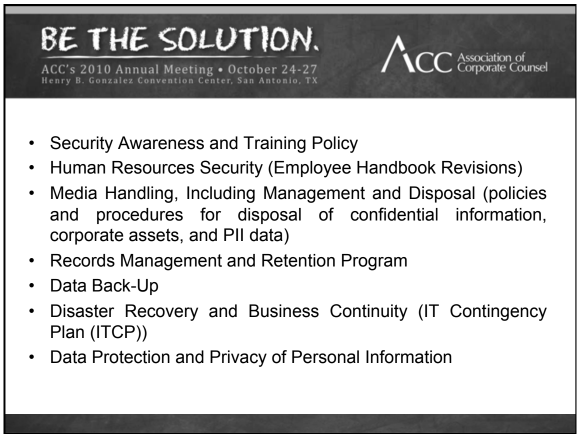
ACC Association of Corporate Counsel

- Access Controls
- Password Policy
- Third- Party Access
- Incident Response Policy (including, Forensic Procedures / Cyber Investigations, Responding to Government Investigations Regarding Security Instance and Loss or Potential Loss of PII)
- Asset Management Policy (Use of Non-1836 Technologies Owned Equipment)
- Systems and Application Monitoring and Logging (1836 Technologies): Internet/Network Usage and Monitoring Policy (US and Europe))



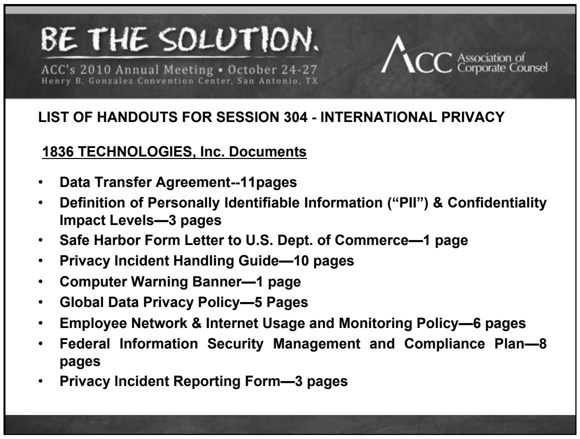
BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

- Configuration Management Policy
- Change Management Policy
- Physical and Environmental Protection Policy
- Security Planning Process
- Systems and Services Development, Acquisition and Life Cycle
- System and Communication Detection Policy
- System and Information Integrity
- Information System Maintenance Encryption Policy
- Certification Accreditation/Security Assessments Policy



BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

- Security Awareness and Training Policy
- Human Resources Security (Employee Handbook Revisions)
- Media Handling, Including Management and Disposal (policies and procedures for disposal of confidential information, corporate assets, and PII data)
- Records Management and Retention Program
- Data Back-Up
- Disaster Recovery and Business Continuity (IT Contingency Plan (ITCP))
- Data Protection and Privacy of Personal Information

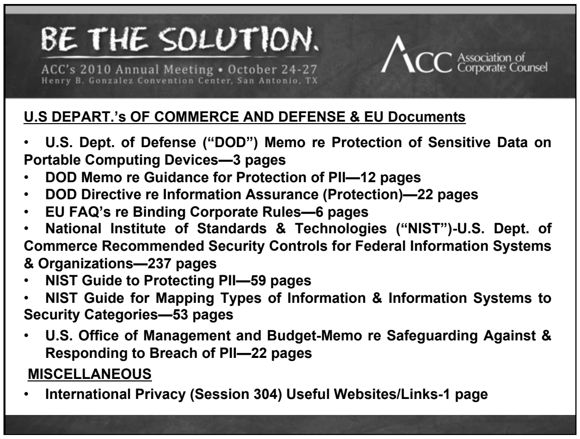


BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

LIST OF HANDOUTS FOR SESSION 304 - INTERNATIONAL PRIVACY

1836 TECHNOLOGIES, Inc. Documents

- **Data Transfer Agreement--11pages**
- **Definition of Personally Identifiable Information ("PII") & Confidentiality Impact Levels—3 pages**
- **Safe Harbor Form Letter to U.S. Dept. of Commerce—1 page**
- **Privacy Incident Handling Guide—10 pages**
- **Computer Warning Banner—1 page**
- **Global Data Privacy Policy—5 Pages**
- **Employee Network & Internet Usage and Monitoring Policy—6 pages**
- **Federal Information Security Management and Compliance Plan—8 pages**
- **Privacy Incident Reporting Form—3 pages**



BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

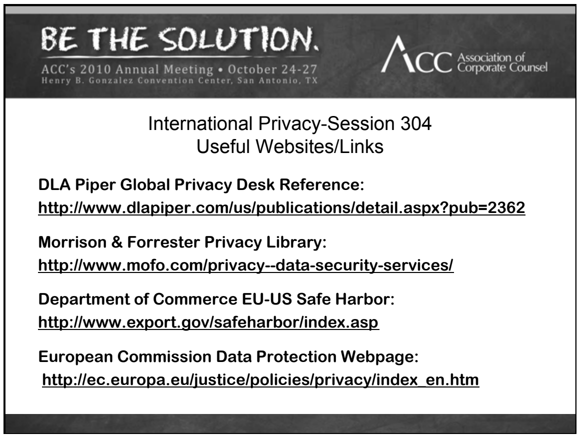
ACC Association of Corporate Counsel

U.S DEPART.'s OF COMMERCE AND DEFENSE & EU Documents

- **U.S. Dept. of Defense ("DOD") Memo re Protection of Sensitive Data on Portable Computing Devices—3 pages**
- **DOD Memo re Guidance for Protection of PII—12 pages**
- **DOD Directive re Information Assurance (Protection)—22 pages**
- **EU FAQ's re Binding Corporate Rules—6 pages**
- **National Institute of Standards & Technologies ("NIST")-U.S. Dept. of Commerce Recommended Security Controls for Federal Information Systems & Organizations—237 pages**
- **NIST Guide to Protecting PII—59 pages**
- **NIST Guide for Mapping Types of Information & Information Systems to Security Categories—53 pages**
- **U.S. Office of Management and Budget-Memo re Safeguarding Against & Responding to Breach of PII—22 pages**

MISCELLANEOUS

- **International Privacy (Session 304) Useful Websites/Links-1 page**



BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

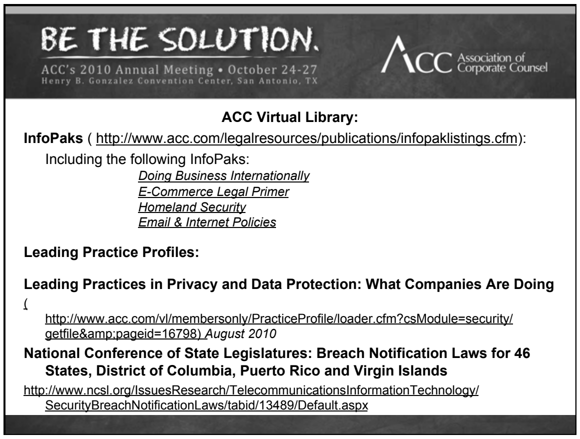
International Privacy-Session 304
Useful Websites/Links

DLA Piper Global Privacy Desk Reference:
http://www.dlapiper.com/us/publications/detail.aspx?pub=2362

Morrison & Forrester Privacy Library:
http://www.mofo.com/privacy--data-security-services/

Department of Commerce EU-US Safe Harbor:
http://www.export.gov/safeharbor/index.asp

European Commission Data Protection Webpage:
http://ec.europa.eu/justice/policies/privacy/index_en.htm



BE THE SOLUTION.
ACC's 2010 Annual Meeting • October 24-27
Henry B. Gonzalez Convention Center, San Antonio, TX

ACC Association of Corporate Counsel

ACC Virtual Library:

InfoPaks (http://www.acc.com/legalresources/publications/infopaklistings.cfm):

Including the following InfoPaks:

Doing Business Internationally
E-Commerce Legal Primer
Homeland Security
Email & Internet Policies

Leading Practice Profiles:

Leading Practices in Privacy and Data Protection: What Companies Are Doing
(http://www.acc.com/vl/membersonly/PracticeProfile/loader.cfm?csModule=security/getfile&amp;pageid=16798) *August 2010*

National Conference of State Legislatures: Breach Notification Laws for 46 States, District of Columbia, Puerto Rico and Virgin Islands

http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

LIST OF HANDOUTS FOR SESSION 304-INTERNATIONAL PRIVACY

1836 TECHNOLOGIES, Inc. Documents

1. Data Transfer Agreement--11pages

2. Definition of Personally Identifiable Information ("PII") & Confidentiality Impact Levels—3 pages

3. Safe Harbor Form Letter to U.S. Dept. of Commerce—1 page

4. Privacy Incident Handling Guide—10 pages

5. Computer Warning Banner—1 page

6. Global Data Privacy Policy—5 Pages

7. Employee Network & Internet Usage and Monitoring Policy—6 pages

8. Federal Information Security Management and Compliance Plan—8 pages

9. Privacy Incident Reporting Form—3 pages

U.S DEPART.'s OF COMMERCE AND DEFENSE & EU Documents

1. U.S. Dept. of Defense ("DOD") Memo re Protection of Sensitive Data on Portable Computing Devices—3 pages

2. DOD Memo re Guidance for Protection of PII—12 pages

3. DOD Directive re Information Assurance (Protection)—22 pages

4. EU FAQ's re Binding Corporate Rules—6 pages

5. National Institute of Standards & Technologies ("NIST")-U.S. Dept. of Commerce Recommended Security Controls for Federal Information Systems & Organizations—237 pages

6. NIST Guide to Protecting PII—59 pages

7. NIST Guide for Mapping Types of Information & Information Systems to Security Categories—53 pages

MISCELLANEOUS

DATA EXPORTER CLIENT

and

1836 TECHNOLOGIES INC.

DATA TRANSFER AGREEMENT

(Model Contract relating to the transfer of personal data outside the European Economic Area) in accordance with European Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593.

THIS AGREEMENT is made on ______ [date].

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection,

IT IS HEREBY AGREED as follows:

1. **Client Legal Name**, a company registered in (company number xxxxxxx), whose registered office is at ____ ("**Company short name**", or the "**data exporter**"); and

2. **1836 TECHNOLOGIES INC.**, a company registered in the USA under EIN _______________, whose registered office is at _________, San Antonio, TX (the "**Supplier**", or the "**data importer**"),

HAVE AGREED on the following Contractual Clauses (the "**Clauses**") in order to implement and assure adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1:

Clause 1

Definitions

For the purposes of the Clauses:

(a) **'personal data'**, **'special categories of data'**, **'process/processing'**, **'controller'**, **'processor'**, **'data subject'** and **'supervisory authority'** shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the **"Directive"**);

(b) **'the data exporter'** shall mean the controller who transfers the personal data, namely Company or such of Company's affiliated companies as may transfer personal data to the data importer;

(c) **'the data importer'** shall mean the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of these Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) **'the subprocessor'** shall mean any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) **'the applicable data protection law'** shall mean the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) **'technical and organisational security measures'** shall mean those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix I which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary Clause

(a) The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

(b) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

(c) The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

(d) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or

subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Co-operation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely ___________________.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[1]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

[1] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely ____________________.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

IN WITNESS WHEREOF, the parties have entered into this agreement on the date first set out above:

Company Legal Name		**1836 Technologies Inc.**
Name:		Name:
Title:		Title:
Date:		Date:

Appendix 1

Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

[***to be included***]

Data importer

The data importer is (please specify briefly your activities relevant to the transfer):

[***to be included***]

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

[***to be included***]

Categories of data

The personal data transferred concern the following categories of data (please specify):

[***to be included***]

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

[***to be included***]

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

[***to be included***]

IN WITNESS WHEREOF, the parties have entered into this agreement on the date first set out above:

Data Exporter **Company Legal Name**		**Data Processer** **1836 TECHNOLOGIES Inc.**
Name:		Name:
Title:		Title:
Date:		Date:

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
………………………………………………………………………………………………..

Agreed as to Appendix 2:

Data Exporter **Company Legal Name**		**Data Processor** **1836 TECHNOLOGIES Inc.**
Name:		Name:
Title:		Title:
Date:		Date:

PRIVILEGED AND CONFIDENTIAL
1836 Technologies, Inc. – ACC Annual Conference - 2010

Definition of Personally identifiable information (PII) and Confidentiality Impact Levels

1. Personally Identifiable Information (PII)

a. PII is generally defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place5 of birth, mother's maiden name, etc."

b. To distinguish an individual is to identify an individual. Some examples of information that can distinguish an individual include, but are not limited to, name, passport number, social security number, or biometric image and template. In contrast, a list containing only credit scores or phone numbers does not have sufficient information to distinguish a specific individual, unless it is linked to or linkable to other secondary information, which when combined are sufficient to distinguish that individual.

c. An individual with access to both databases may be able to link together information from the two databases and distinguish individuals.

- Liked data: If the secondary information source is present on the same system or a closely-related system, then the data is considered *linked*.
- Linkable data: If the secondary source is available to the general public or can be obtained, such as from an unrelated system within the organization, then the data is considered *linkable*.

d. The following list contains *examples* of information that may be considered PII.

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as SSN, passport number, driver's license number, taxpayer identification number, patient identification number, government service serial number, and financial account or credit card number
- Security clearance or Military Service information, such as service, serial number, or rank
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Address information, such as street address or email address, or telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scans, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration or identification number, and title numbers and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, ethnicity, immigration status, sexual orientation, or credit scores, employment, medical, education, or financial information)

2. Impact Levels (Low, Medium, and High)

Not all PII must be protected to the same degree and//or require the same security controls to protect the integrity and availability of the PII. 1836 Technologies will assign security controls based on the level of harm caused from a loss of the PII due to a security breach.

a. There are three *impact levels*: Low, Moderate, and High:

"The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm or inconvenience to individuals.

The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries." [1]

b. *Examples* of harm to individuals as described in these impact levels:

i. A breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing a telephone number.

ii. A breach of PII at the moderate impact level would include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail.

iii. Harm at the high impact level involves serious physical, social, or financial harm, resulting in potential loss of life or inappropriate physical detention.

3. Factors to consider when determining Impact levels.

1836 Technologies will consider these factors when determining the PII confidentiality Impact Level:

i. *Ability to Distinguish individuals*. This factor looks at how easily the PII can be used to distinguish a particular individual. For example SSN's fingerprints, and names are uniquely

[1] These definitions are taken from the NIST Guide to Protecting the Confidentiality of PII – NIST SP 800-122 (Draft)

identifiable PII, whereas phone numbers alone or gender may not distinguish an individual without other information.

ii. *Use of PII alone or in the aggregate may affect and/or alter the Impact level to be assigned to the PII*. This factor looks at how the PII is stored. For example, while a list containing just SSNs would be assigned a moderate impact level, a list of SSNs with name, mother's maiden name, and address, would be assigned a High impact level. Also consider linkability of these Data Fields when assigning impact levels.

iii. *Context of Use*. This factor looks at the purpose for which the PII collected, stored, used, processed, disclosed, or disseminated, as well as how that PII is used or could potentially be used. For example, is the PII used to determine eligibility for employment, benefits, or security clearance, or for payroll or tax purposes.

iv. *The legal obligations that apply to the PII and/or 1836 Technologies*. This factor looks at whether there are contractual or legal, obligations that impact on either the PII or 1836 Technologies. These obligations can be found in Contract or government laws, regulations, or directives (these can be found at the international, federal, or state level), and can result in civil and criminal fines for non-compliance.

v. *The nature and scope of authorized access to the PII*. This factor looks at how widely the PII may be accessed within 1836 Technologies. The more wide the nature and scope of access, the higher the impact level must be to mitigate the increased risk caused by the wide access to the PII.

4. Identifying PII

The task of identifying PII and/or locating PII within our client's databases and/or our own network can be a daunting task. 1836 Technologies will use a variety of methods to identify all PII residing within our network or that is placed under our control, commonly referred to as Privacy Threshold Analysis, identifying PII clauses in all RFPs and Contracts to assess any contractual or legal requirements for handling the PII. If you are not sure whether information is PII, the Impact Level to be assigned to the PII, you are to contact the ____ within your Sector, or the ______ [Privacy Official].

5. Incident Response for Breaches of PII

Breaches involving PII can trigger Contractual and legal obligations to notify the Government and/or the data subjects whose PII has been comprised. In addition to the potential harm to the data subject, such breaches can receive considerable media attention, which can cause harm to 1836 Technologies's reputation. To protect 1836 Technologies, its employees, and data subjects, and to comply with applicable legal and contractual obligations, 1836 Technologies has developed policies and a Privacy Incident Handling User's Guide for breaches of PII. This Guide is posted on 1836 Technologies's Privacy Reporting Portal, and includes a Privacy Incident Checklist, and Identify Theft Risk Evaluation.

6. Role of 1836 Technologies Privacy _______

1836 Technologies has established a Privacy [Division] that will be responsible for handling all Breaches of PII. The Privacy [Division] will be comprised of representatives from ___ [_____, IA, ITS, and Legal. 1836 Technologies Personnel are responsible for immediately notifying the Privacy _____ of all breaches of PII.

Date

Mr. _______________
U.S. Department of Commerce
Room 2003
14th & Constitution Avenue, N.W.
Washington, D.C. 20230.

Re: Re-affirmation of Safe Harbor Certification for 1836 Technologies, Inc.

Dear Ms. _________:

I hereby affirm that I am the officer who is authorized to certify 1836 Technologies's continued adherence to the Safe Harbor framework. I understand that any misrepresentations could be actionable against 1836 Technologies, and that a failure to adhere to the Safe Harbor framework may lead to enforcement actions by the relevant authorities. Therefore, pursuant to the EU-U.S. Safe Harbor framework, 1836 Technologies wishes to reaffirm and verify its certification of its compliance with the Safe Harbor requirements.

In compliance therewith, 1836 Technologies certifies that the information previously submitted to the Department of Commerce regarding its published privacy policy concerning its care and use of personal information received from the EU has been implemented, is prominently displayed by 1836 Technologies, and is accessible to its employees. 1836 Technologies further certifies that its privacy policy conforms to the Safe Harbor principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that 1836 Technologies has in place procedures for training employees in its implementation, and disciplining them for failure to follow it; and that 1836 Technologies has in place internal procedures for periodically conducting objective reviews of compliance with the above.

If you have any questions or would require further information, please do not hesitate to contact me.

Yours sincerely,

1836 TECHNOLOGIES, INC.

PRIVACY INCIDENT HANDLING GUIDANCE

DESKTOP USER'S GUIDE

DRAFT – PRIVILEGED & CONFIDENTIAL

OUTLINE, PRIVACY INCIDENT CHECKLIST & QUESTIONNAIRE

PURPOSE OF THIS GUIDE

This guide provides important information about privacy incidents, including how to identify a privacy incident and what procedures to follow to correctly respond to a potential privacy incident.

1836 Technologies employees, consultants, subcontractors, and temporary staff must follow the steps outlined in this guide when investigating or responding to any privacy incident.

This guide also provides important privacy information for Project Managers. Project Managers should consider privacy from the proposal process through the end of a project. 1836 Technologies must abide by all federal privacy regulations and agency guidance. This Privacy guidance includes Initial and periodic briefings the individual and corporate responsibilities identified in FAR clause 52.205-2, Security Requirements; 52.223-6, Drug Free Workplace; 52.225-2, Privacy Act; and 52.239-1, Privacy or Security Safeguards. Each employee is also required to complete initial and annual Privacy training such as those required of National Industrial Security Program Operating Manual (NISPOM) Chapter 3.

This guide shows 1836 Technologies commitment to privacy and ability to respond to privacy incidents in an organized and efficient manner.

For more information, visit the Privacy Portal at ____________.

TABLE OF CONTENTS

Privacy Incident Checklist

Reporting (Section 5): Upon detecting an incident that may involve PII	
Responsible Party	**Action Item**
[Name of Company] personnel who detected the incident	Initiate the [Name of Company] Online Incident Handling report and\or notify the Task Lead or Project Manager (PM) of the suspected or confirmed incident. If the PM is not available, [Name of Company] personnel contacts the Name of Responsible Party.
Task Lead or PM	Ensure accuracy in the [Name of Company] Online Incident Handling report; or initiate the report if it was not initiated by the employee. Send the report to the Privacy Division.
Name of Responsible Party	Send the Privacy Incident Notification to the [Name of Company] COO and CEO.
Name of Responsible Party	Notify the [Name of Company] Chief Financial Officer (CFO) of any Privacy Incident involving financial systems.
[Name of Company] CFO	Notify the issuing bank(s) of the incident as appropriate.
Name of Responsible Party	Supplement the Privacy Incident Report to reflect the CFO's notification of the issuing bank(s), if needed.
Name of Responsible Party	Notify the [Name of Company] Chief of Security when the incident involves security-related issues affected [Name of Company] personnel, property, facilities, and information.
Name of Responsible Party	Consult with the CIO if the incident impacts the security of an [Name of Company] IT system.
Name of Responsible Party	Supplement the Privacy Incident Report at the **[Name of Company] Privacy Incident Reporting Portal** as needed.
Risk Analysis (Section 6)	
Responsible Party	**Action Item**
Name of Responsible Party	Conduct a risk analysis of the incident and documents the analysis in the Identity Theft Risk Evaluation in the [Name of Company] Online Incident Reporting System.
Name of Responsible Party	Immediately evaluate the context of the incident and the PII that was potentially or actually lost or compromised.
Name of Responsible Party	Identify the type of risk involved in the incident.
	The Name of Responsible Party evaluates whether the data elements constitute the type of information that may pose a risk of identity theft (e.g., types include: (1) SSN; or (2) name, address, or telephone number combined with: (a) any identification number; (b) biometric record; (c) financial account number together with a PIN or security code (if a PIN or security code is necessary to access the account); or (d) any additional specific factor that adds to the personally identifying profile of a specific individual; (3) date of birth, password, and mother's maiden name); or (4) Sensitive PII, such as SSN, driver's license number; financial account number; citizenship or immigration status; or medical information. € If the Name of Responsible Party neither suspects nor confirms that identity theft is implicated, then the Name of Responsible Party proceeds with the evaluation of the five factors determining the likely risk of harm. € If identity theft is implicated, the Name of Responsible Party immediately completes the Identity Theft Risk Evaluation.

	Name of Responsible Party evaluates the five factors to determine the likely risk of harm posed by the Privacy Incident: □ The nature of the data elements involved; □ The number of individuals affected; □ The likelihood the PII is accessible and usable; □ The likelihood the Privacy Incident may lead to harm; ▪ Where criminal activity is suspected or confirmed, the Name of Responsible Party will determine whether to contact law enforcement. □ The ability to mitigate the risk of harm.	
	Name of Responsible Party	Assign an impact level of low, moderate, or high to each risk factor.
	The likely risk of harm is LOW where the risk of identity theft or other harm is unlikely (e.g., the compromise of the PII could not lead to identity theft or other risk of harm; the PII has been recovered and determined that there was no access or distribution of information; the PII was encrypted. The likely risk of harm is MODERATE or HIGH where criminal activity is suspected or confirmed. € Name of Responsible Party will ensure external notification of law enforcement for incidents that do not impact physical security; such notification should be handled in consultation with the [Name of Company] Chief of Security. € If criminal activity impacts physical security, the Name of Responsible Party, in coordination with the [Name of Company] Chief of Security, will determine whether to contact law enforcement. € Notification and involvement of external law enforcement must be documented in the Privacy Incident Report. All Sensitive PII must be designated as MODERATE or HIGH impact.	
	Name of Responsible Party	If the incident involves financial data, consult with the [Name of Company] CFO on how to proceed.
	Name of Responsible Party	If the incident involves security-related issues affecting [Name of Company] personnel, property, facilities, and information, then work with the [Name of Company] Chief of Security
	Name of Responsible Party	Make a preliminary recommendation as to whether notification is warranted and works with [Name of Company] Communications and Public Affairs.
	Name of Responsible Party	Recommend notification where there is a reasonable risk of harm and the decision will not lead to the overuse of notification.
	Name of Responsible Party	Identify the steps [Name of Company] should take to mitigate the risk of harm.
	Name of Responsible Party	Attach the Identity Theft Risk Evaluation to the Privacy Incident Report.
	Name of Responsible Party	Notify the COO and CEO.

Investigation (Section 7)		
	Name of Responsible Party	Limit internal notifications and access to individuals who have a legitimate need to know.
	Name of Responsible Party	Review what has happened as follows: □ Document the investigation and gather all information necessary to describe and address the incident. □ Confirm what personal information is lost or at risk. □ Identify the steps taken to reduce the risk of harm.
	[Name of Company] Πριϖαχψ ∆ιϖισιον	Follow the [Name of Company] internal incident handling procedures: □ Identify what further steps must be taken for the formulation of any further response by SRA. □ Analyze the precedents and indications regarding computer security. □ Identify information resources that have been affected and identify additional resources that might be affected. □ Estimate the current and potential technical impact (e.g., data, database, system or network) of the incident. □ Back up the system in accordance with the standards and procedures set forth in [Name of Company] 4300A, Sensitive Systems.
	Name of Responsible Party	Adhere to standard investigation procedures.
	Name of Responsible Party	Create and maintain a complete record of the investigation.
	Name of Responsible Party	Protect and preserve all evidence as follows: □ Consult with Name of Responsible Party to address issues pertaining to the handling of evidence and chain of custody. □ Take precautions to prevent destruction or corruption of evidence that may be needed to support criminal prosecution. □ Identify and properly secure all evidence to maintain its validity in court.
	Name of Responsible Party	□ Create and maintain a chain of custody log of all personnel who have access to the evidence. □ Keep a record of the individuals who have touched each piece of evidence, and the date, time, and locations where the evidence is stored. □ Protect the chain of custody of the backup data. □ Store the data in a secure location.
	Name of Responsible Party	Review events and actions at the conclusion of an incident and make recommendations regarding any indicated changes in the [Name of Company] technology and incident handling plan.
	Name of Responsible Party	Upon completion of the investigation, update the Privacy Incident Report at the **[Name of Company] Privacy Incident Reporting Portal** to indicate the closure of the investigation.

Notification (Section 8)		
	Name of Responsible Party	Consulting with [Name of Company] Communications and Public Affairs, assess the likely risk of harm posed by the incident and consider external notification. Make a final decision as to whether, how and when external notification will be provided.
	Name of Responsible Party	If the Name of Responsible Party determines that external notification is warranted, prepares a proposed draft notification letter (without any PII concerning the affected individuals included in the draft) and proposed draft/press release (if any) for consideration by the Component Head.
	Name of Responsible Party	Send notification letters to affected third parties.
	Name of Responsible Party	Attach the notification documents to the Privacy Incident Report in the **[Name of Company] Privacy Incident Reporting Portal** (e.g., External Notification Assessment, press release, notification letter to affected individuals).
Mitigation (Section 9)		
	All	Work to prevent or minimize any consequent harm.
	PM	Gather, secure, and document evidence of the incident.
	Name of Responsible Party	Work with the Computer Support Team regarding containment measures.
	Name of Responsible Party	Work with the Computer Support Team to manage and contain the incident.
	Name of Responsible Party	Work with the Computer Support Team to implement actions to correct and prevent further risks stemming from the incident.
	Name of Responsible Party	Secure paper records, if applicable.
	Name of Responsible Party	Work with the Computer Support Team to identify and mitigate exploited vulnerabilities.
	Computer Support Team	Remove malicious code or compromised or inappropriate materials from the network (including intranet) and/or Internet.
	Computer Support Team	Return affected systems to an operationally ready state and confirm that the affected systems are functioning normally.
	Name of Responsible Party	Restore security measures protecting paper information, if applicable.
	Name of Responsible Party	Consider countermeasures as dictated by the nature and sensitivity of the PII, including but not limited to: □ Notifying affected individuals, the public, and other government entities (Section 8); □ Offering credit monitoring services to mitigate the misuse of the PII and identify patterns of suspicious behavior; □ Removing information from an Internet or intranet page; □ Notifying the Chief of Security if criminal activity is suspected or confirmed and consultation to determine whether law enforcement should be notified; and □ Notifying CFO in order for the CFO to notify the issuing bank for incidents involving credit cards (Sections 5 and 6).
	[Name of Company] IT Security Entity and Name of Responsible Party	Document all implemented mitigation measures in the Privacy Incident Report.

Consequences and Accountability (Section 10)		
	[Name of Company] Human Resources	Decide on disciplinary action to be taken if the privacy incident involves wrongdoing or negligence.
Closure of Privacy Incidents (Section 11)		
	Name of Responsible Party	Update the incident report at the [Name of Company] Privacy Portal to recommend incident closure.
	Name of Responsible Party	Make closure recommendation in weekly status reports of ongoing Privacy Incidents.
	Name of Responsible Party	Issue closure notifications to [Name of Company] COO, CEO, and other personnel involved in the incident.
Supplemental Activities (Sections 5.6, 8.1.2, 11, and 12)		
	Name of Responsible Party	Issue weekly status report of ongoing incidents to senior management.
	Name of Responsible Party	Identify and posts lessons learned.
	Name of Responsible Party	Review implementation of Privacy Incident Handling Guidance annually or more frequently.

Identity Theft Risk Evaluation

Identity Theft Risk Evaluation	
Factor	**Identify Risk Level (e.g., Low, Moderate, High) and Provide Brief, Specific Explanation**
Nature of data elements involved	1. Consider the data elements in context. Are the compromised data elements PII? Yes □ No □ 2. Explain:
Number of individuals affected	3. Is there a way to identify the number of the individuals impacted by the incident? (For example, is there a recent computer backup of all information or is there a hard copy of the information?) Yes □ No □ 4. Identify the total number of affected individuals (if known): 5. Explain how the identity of affected individuals is known:
Likelihood PII is accessible and usable	6. Is the information □ electronic or □ hardcopy? 7. How difficult would it be for an unauthorized person to access this information? 8. Was it locked or secured? Yes □ No □ 9. If it was secured, identify what physical or electronic protections for electronic or hardcopy were used: 10. Summarize the risk of whether an unauthorized individual will know the value of the information and either use the information or sell it to others.
Likelihood incident may lead to harm	11. Will substantial harm, embarrassment, inconvenience, or unfairness occur from this loss? Yes □ No □ Explain why. 12. Determine the likelihood the incident is the result of or could result in criminal activity. Focus on the means the loss or compromise of PII occurred. 13. Was it the result of a criminal act (e.g., PII stolen targeting the data such as a computer hacker)? Yes □ No □ 14. Is it likely to result in criminal activity? Yes □ No □ 15. Was the storage device, rather than the PII itself, the target of the theft?

	Yes □ No □ 16. Is there evidence that the compromised information is being used to commit identity theft? Yes □ No □ **17. NOTE: If the answer is yes to any of these questions, the Privacy Division should categorize the incident as either a Moderate- or a High-Impact Privacy Incident. Under these circumstances, the Name of Responsible Party will ensure external notification of law enforcement for incidents that do not impact physical security; such notification should be handled in consultation with the [Name of Company] Chief of Security.**
Ability to mitigate risk of harm	18. Explain the extent to which the agency has the capabilities to take countermeasures: 19. Does the incident involve government-authorized credit cards? Yes □ No □ 20. If so, has [Name of Company] notified the issuing bank? Yes □ No □ 21. Does the incident involve individuals' bank account numbers used for the direct deposit of credit card reimbursements, employee salaries, or any benefit payment? 22. Yes □ No □ 23. Has [Name of Company] notified the bank or other entity that handles that particular transaction for SRA? Yes □ No □ 24. Can [Name of Company] monitor and prevent attempts to misuse the covered information? 25. Yes □ No □ 26. Can the compromised information be used to open new accounts? 27. Yes □ No □ 28. If so, is data breach monitoring be appropriate (e.g., volume of persons affected or law enforcement evidence)? Yes □ No □ 29. Would credit monitoring be more appropriate? Yes □ No □ 30. Have appropriate law enforcement agencies been contacted to participate in the investigation of the incident? Yes □ No □ If so, state who has been contacted.

PRIVILEGED & CONFIDENTIAL

1836 Technologies Computer Warning Banner - Draft – ACC National Conference 2010

Version 1 of Warning Banner:

"This computer and 1836 Technologies's network and connected systems, and storage media (hereinafter 1836 Technologies's IT System) are for official use by authorized personnel only. Their proper use is subject to 1836 Technologies's Information Security Policies. All activities may be monitored, recorded, or copied by authorized personnel. Any data or information stored on or sent over 1836 Technologies's IT System may be used by the company as part of any internal investigations, disciplinary proceedings, and/or provided to law enforcement officials. Failure to use 1836 Technologies's IT System in accordance with 1836 Technologies's policies, rules, and regulations may result in the revocation of your right to utilize 1836 Technologies's IT Assets, and/or be grounds for discipline, up to and including termination." Users shall have no expectation of privacy with respect thereto, and your use of 1836 Technologies's IT system constitutes consent to these conditions.

Version 2

1836 Technologies's IT System and IT assets are for 1836 Technologies work-related use only and will be subject to 1836 Technologies's Information Security Policies. All activities may be monitored, recorded, and copied by authorized 1836 Technologies ITS personnel. Any data or information stored on 1836 Technologies's IT assets or sent over 1836 Technologies's IT System may be used by the company as part of any internal investigation or disciplinary proceeding, and/or provided to law enforcement officials. Failure to use these IT assets in accordance with 1836 Technologies policies, rules, and regulations may result in disciplinary actions, up to and including termination. Users shall have no expectation of privacy with respect thereto, and your use of 1836 Technologies's IT system constitutes consent to these conditions.

Version 3

This computer, network and connected systems are for 1836 Technologies work-related use only, and users shall have no expectation of privacy with respect to their use. Any failure to comply with 1836 Technologies Information Security policies may result in disciplinary actions, up to and including termination. User understands that any data stored or sent over 1836 Technologies's IT system may be used and monitored by 1836 Technologies. Your use of 1836 Technologies's IT system constitutes consent to these conditions.

	POLICY
DATA PRIVACY POLICY	Number-Version: ________
Approved:	Effective Date: ______, 20__
	Supersedes: _________
Title:	Page 1 of 5

PURPOSE

1836 Technologies collects and uses personal data to provide world-class services for our employees, clients, and partners. This Policy is designed to set forth how 1836 Technologies will handle personal data that it collects in the normal course of business. 1836 Technologies strives to be global and consistent in how it handles personal data. Our privacy policy applies to:

1. All individuals who provide personal information, such as consumers, customers, research subjects, business partners, shareholders, job applicants, employees, retirees and others;
2. All locations where we operate, even where local regulations do not exist; and
3. All methods of contact, including in person, written, via the Internet, direct mail, telephone, or facsimile.

This Policy describes 1836 Technologies' standard global procedure governing access to and use of 1836 Technologies' Personal Data across borders. As part of this Policy, 1836 Technologies will comply in all material respects with the European Union Privacy Directive (Directive 95/46/EC) and implementing legislation enacted by the member states of the European Union with respect to its operations in those member states; as well as such legislation as the Health Insurance Portability and Accountability Act of 1996, as amended, and other privacy laws, rules, and regulations that may apply to 1836 Technologies, its employees, or its clients in those countries where 1836 Technologies has operations.

This Policy does not necessarily describe how local management may handle personal data in order to comply with local privacy laws. Local management in conjunction with the responsible human resources manager(s) will be responsible for accessing and complying with local/unique laws and/or rules regarding the processing of personal information in that particular locale.

This Policy is also designed to inform all employees about their obligation to protect the privacy of all individuals (whether co-employees, independent contractors, or sub-contractors) and the security of their personal information. The violation of this Policy, whether negligent or intentional, will be subject to disciplinary action by 1836 Technologies.

SCOPE

This is a Global Policy. 1836 Technologies will extend the protection of the Safe Harbor Privacy Principles to all personal data originating outside of the United States, and which is transferred to 1836 Technologies facilities in the United States. Outside of the United States, 1836 Technologies facilities are required to comply with this Policy as well as the privacy laws in force in their local jurisdictions

DEFINITIONS

"Controller," in this case, refers to 1836 Technologies and its authorized s, which determine the purposes and means of processing of Personal Data.

"Data Subject" in this case refers to any employee or third person (e.g., consultant or independent contractor) who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

DATA PRIVACY POLICY	POLICY	
	Number-Version:	________
Approved:	Effective Date:	______, 20__
	Supersedes:	________
Title:	Page 2 of 5	

"General Business Purpose" means the Processing of Personal Data for any activity related to the commercial operations of 1836 Technologies' worldwide organization. This could include, but is not limited to its sales, marketing, and research and development operations; protecting intellectual property; the provision of services; internal operations; and general employment matters, including recruitment both internally and externally. Data processing for General Business Purposes includes, but is not limited to, publishing global directories, maintaining files, payroll processing, managing benefit and medical plans, conducting performance reviews, and intra-company communications.

"Personal Data" means any information related to an identified or an identifiable person. For example, a Data Subject's home address, e-mail address and/or phone number, personnel file, or benefits information would constitute Personal Data.

"Processor" means a natural or legal person, or any other entity that processes Personal Data on behalf of the Controller and under its control. In this context, a Processor may be a payroll preparation firm that works on behalf of 1836 Technologies and under its control. 1836 Technologies requires Processors to protect the privacy, confidentiality and security of 1836 Technologies Personal Data.

"Processing" of Personal Data means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"1836 Technologies" means ____________, as well as its affiliated and subsidiary companies within the Group.

"Sensitive Data" is a subset of Personal Data, and refers to any Personal Data pertaining to racial or ethnic origins, trade union membership, medical or health conditions, political or religious beliefs, sex life, or criminal history.

"Third Party" means any natural or legal person, public authority, agency or any other entity other than the data subject, the Controller, the Processor and the persons who, under the direct authority of the Controller or the Processor, are authorized to process the Personal Data.

GENERAL

1836 Technologies Global Data Privacy Policy ("Policy") has been designed to comply with the Safe Harbor Privacy Principles. The European Commission has determined that U.S. based companies that comply with the Safe Harbor Privacy Principles provide an adequate degree of privacy protection. Accordingly, transfers to 1836 Technologies facilities in the United States satisfy the requirements of the EU Directive on Data Protection (Directive 95/46). For more information about the Safe Harbor Privacy Principles and to view our certification, visit the U.S. Department of Commerce's Safe Harbor Web site [add hyperlink]. If you would like to contact us directly about the Safe Harbor program, please send an e-mail to _____@xyz.com.

How We Use and Safeguard Personal Data

A Data Subject's Personal Data is initially maintained in his/her personnel file and/or entered into _______and/or _______ databases; which are managed by 1836 Technologies' local Human Resource Managers. Thereafter, in the course of day-to-day business operations, authorized individuals within

DATA PRIVACY POLICY	POLICY
	Number-Version: ________
Approved:	Effective Date: ______, 20__
	Supersedes: ________
Title:	Page 3 of 5

1836 Technologies may from time to time utilize and/or transfer the Data Subject's Personal Data among various 1836 Technologies worldwide locations. These international transfers of Personal Data are necessary in order to carry out 1836 Technologies' General Business Purposes. To safeguard this Personal Data, and to comply with current legal requirements, 1836 Technologies has formalized and implemented a standard global procedure governing access to and use of Personal Data across borders.

POLICY

Quality of Personal Data

1836 Technologies will take reasonable steps that Personal Data and Sensitive Data are:

a. Obtained, where possible, directly from the Data Subject to whom the Personal Data relates;

b. Obtained and processed fairly and lawfully by 1836 Technologies for and General Business Purposes;

c. Relevant to and no more revealing than is necessary for General Business Purposes; and

d. Kept up to date to maintain data accuracy, while data are under the control of 1836 Technologies, and kept only for so long as is reasonably necessary.

Notice and Use of Personal Data

1836 Technologies informs Data Subjects what information we collect, how it is used, whether it may be temporarily transferred to others to provide the products or services requested and how to contact 1836 Technologies with privacy inquiries. 1836 Technologies' use of Personal Data and Sensitive Data will be limited to General Business Purposes, and will not be kept longer than is necessary.

Individual Rights of Access to Personal Data

1836 Technologies takes steps to make sure that the personal information it uses is correct. 1836 Technologies will allow Data Subjects reasonable access to Personal Data and Sensitive Data about themselves during normal working hours and upon reasonable request, and will be allowed to update and/or correct any inaccurate information.

Security of Personal Data

1836 Technologies will take reasonable precautions to protect Personal Data and Sensitive Data from loss, misuse, unauthorized access, disclosure, alteration and destruction. For these purposes, 1836 Technologies will classify such data into three levels of security within 1836 Technologies:

a. Level 1 (known as "1836 Technologies Public Data")

This is Personal Data such as job title, workplace location, office telephone number and/or e-mail address. 1836 Technologies Public Data will be available for unrestricted use within 1836 Technologies and/or to Processors. 1836 Technologies Public Data may be disclosed outside of 1836 Technologies for General Business Purposes.

b. Level 2 (known as “1836 Technologies Private Data”)

This is Personal Data such as an the data subject’s home contact information, e.g., home address, home e-mail address, and home telephone number, as well as information about compensation and benefits, performance evaluations, and identification numbers. 1836 Technologies Private Data can only be disclosed for General Business Purposes to authorized personnel within 1836 Technologies and to Processors who are authorized to access and/or use such 1836 Technologies Private Data on behalf of a 1836 Technologies business unit. It will be disclosed to Third Parties only with the prior written permission of the concerned, except as may be allowed under EU law or the Safe Harbor Principles.

c. Level 3 (known as “1836 Technologies Sensitive Data”)

Sensitive Data will be treated as highly-restricted data by 1836 Technologies and will be stored locally. Transfers of 1836 Technologies Sensitive Data, either outside the country of origin or outside of 1836 Technologies, will occur only as required for General Business Purposes. Recipients of 1836 Technologies Sensitive Data may include authorized 1836 Technologies Users or Processors who are authorized to access and/or use such Sensitive Data by a Controller authorized to have access to such 1836 Technologies Sensitive Data. 1836 Technologies Sensitive Data will be disclosed to Third Parties only with the prior written permission of the Data Subject, except as may be allowed under EU law or the Safe Harbor Principles.

Accountability

1836 Technologies expects its employees, independent contractors, subcontractors, and partners to maintain the trust placed in 1836 Technologies by those Data Subjects who provide personal information to 1836 Technologies. 1836 Technologies will provide privacy training to its employees to highlight the importance of privacy in its global business conduct program. Those who manage personal information will complete periodic privacy self assessments to make sure that personal information is secure and protected. 1836 Technologies will periodically audit privacy compliance, and where necessary, will extend by contract its privacy policies and data protection practices to 1836 Technologies’ supplier and partner relationships.

Procedure for Accessing Personal Data

1836 Technologies s must receive specific authorization in order to access Personal Data and Sensitive Data classified as Level 2 and above, except when a Data Subject requests access to his or her own data. Questions about Personal Data and/or authorization to access such Personal Data are to be directed to Data Subject’s [e.g., human resources manager]. Unauthorized access may be grounds for disciplinary actions, including termination.

Transfer of Data

Subject to this policy, 1836 Technologies may from time to time transfer Personal Data and Sensitive Data within and between its various worldwide locations for General Business Purposes, in compliance with country of origin regulations, EU law, and the Safe Harbor Privacy Principles and this Policy.

DATA PRIVACY POLICY	POLICY
	Number-Version: ________
Approved:	Effective Date: ______, 20__
	Supersedes: ________
Title:	Page 5 of 5

1836 Technologies' personnel, outside firms and consultants, and clients who receive Personal Data may be located in the Data Subject's home country, the United States or any other country in which 1836 Technologies or its affiliates do business. Therefore, Personal Data may be transferred to any country in the world, including but not limited to __________, the United States of America, and other countries where 1836 Technologies does business, and where the privacy laws may be more or less protective than the privacy laws where the Data Subjects live or work.

Concerned individuals may withhold their consent to such international transfers, and are to be informed of the impact such opt-out will have on their employment within 1836 Technologies (e.g., inability to process benefits or payroll data in a timely or appropriate fashion).

Status of Policy

This policy is subject to change, although 1836 Technologies will provide updates from time to time about changes to this policy. In case of the sale of the company, acquisition or merger, bankruptcy or other change in corporate status, this Policy could change. In addition, this Policy may be supplemented by other company policies and statements.

For More Information

Questions or concerns about how 1836 Technologies handles Personal Data, are to be directed to the Data Subjects supervisor or in-country human resources manager. If the human resource manager cannot answer the question, it will be directed to the Director of ______________.

DRAFT – PRIVILEGED & CONFIDENTIAL

1836 Technologies International Employee Network and Internet Usage and Monitoring Policy

1. Policy Statement

1.1 This policy sets out rules that all 1836 Technologies personnel must follow when using the 1836 Technologies Network and/or the Internet from any 1836 Technologies computer, which includes usage of both the World Wide Web (www) and 1836 Technologies's internal intranet systems(“1836 Technologies Network”)

1.2 This policy also applies to personal use of 1836 Technologies's E-mail (Outlook) system. However, additional confidentiality and liability conditions apply to e-mails.

1.3 This policy also explains what 1836 Technologies may do as an employer to lawfully monitor and report use of the 1836 Technologies Network and/or 1836 Technologies computer and investigate suspected systems breaches by personnel or third parties as well as unlawful behavior.

1.4 This policy applies to any person who uses 1836 Technologies's network and/or computers to access the Internet and E-mail. Where the policy refers to “personnel” or “user” this means anyone employed by 1836 Technologies or its parent company, any person carrying out work activities on 1836 Technologies occupied premises who is not directly employed by 1836 Technologies (e.g. students, interns, work placements or volunteers), or any person providing a service to 1836 Technologies under contract (independent contractor, consultant, or temporary employee). Collectively referred to as “1836 Technologies Personnel”.

1.5 Access to the 1836 Technologies network and/or Internet access is provided primarily to 1836 Technologies personnel to use for 1836 Technologies's business and to develop the skills and knowledge of 1836 Technologies's workforce to the benefit of its business objectives. A certain amount of limited and responsible personal use is also permitted.

1.6 The wide range of information available on the 1836 Technologies Network, as well as the Internet, and the nature and risks associated with the use of the Internet raises concerns about security, integrity, confidentiality, monitoring and proper conduct.

1.7 Data Protection Statement.

1.7 1836 Technologies will monitor all user activity on the Internet at network level for the purposes specified in Section 4.1. Information recorded as part of this automated monitoring process includes user identification, domain names of websites visited, duration of visits, and files uploaded to or downloaded from the Internet. Staff must be made aware that this monitoring may reveal sensitive data about them, for example visits to websites which details the activities of a particular political party or religious group might indicate the political opinion or religious belief of that staff member, or self-help or health advice sites might identify a physical or mental health condition. By carrying out such activities using 1836 Technologies's Internet access facilities, Staff consent to 1836 Technologies processing any sensitive personal data about them that may be revealed through monitoring.

Personnel who do not consent must take responsibility for the maintenance of their own personal privacy by not using 1836 Technologies systems to access this type of information.

2.0 Purpose

The purpose of this policy is to define standards for systems that monitor and limit web use from any computer or host within 1836 Technologies's network. These standards are designed to ensure that 1836 Technologies assets network, and Internet are used in a safe and responsible manner, to ensure the confidentiality, integrity, and reliability of the 1836 Technologies network, and to prevent intrusions into 1836 Technologies's network, breaches of personal and sensitive data, and ensure that employee web use by Personnel be monitored or researched in the event of an incident.

3.0 Scope

This policy applies to all 1836 Technologies employees, contractors, vendors, users, and agents with a 1836 Technologies-owned, contractor provided, government furnished or personally-owned computer or workstation connected to the 1836 Technologies network. This policy applies to all end user initiated communications between 1836 Technologies's network and the Internet, including web browsing, instant messaging, file transfer, file sharing, and other standard and proprietary protocols. Server to Server communications, such as SMTP traffic, backups, automated data transfers or database communications are excluded from this policy.

This policy also explains what 1836 Technologies may do as an employer to lawfully monitor and report use of the system and investigate suspected systems breaches by Personnel or third parties as well as unlawful behavior.

4.0 Policy

4.1 Internet and Network Monitoring

4.1.1 1836 Technologies's Information Technology Services (ITS) Group has incorporated intrusion detection capabilities into its Network so as to provide information relating to unauthorized or irregular behavior on any 1836 Technologies computer, network, or telecommunication system, and analyzing them for signs of possible incidents, which are violations or imminent threats or violation of computer security policies, acceptable use policies, or standard security practices. This is done to protect 1836 Technologies and customer resources and data maintained or stored on 1836 Technologies's network.

4.1.2 To protect the integrity of 1836 Technologies's Network and the data maintained on its Network, the (ITS) Group will monitor Internet usage, network traffic on the 1836 Technologies Network a well as all 1836 Technologies computers and devices, whether or not connected to the 1836 Technologies Network

4.1.3 Because information recorded by the automated monitoring systems can be used to identify an individual user and show, for example, a website or document that a user has been viewing and the time spent browsing, personnel must not assume privacy in their use of the 1836 Technologies's systems, even when accessing the systems in their personal time i.e. out of paid working hours.

4.1.4. In the event that ITS finds inappropriate activity or infestation of a company asset, this information may then be shared with the appropriate 1836 Technologies management, the Incident Response Team, and the Legal Department. 1836 Technologies reserves the right to carry out detailed inspection, make a copy of any 1836 Technologies asset or devices containing 1836 Technologies data, where warranted, and to re-image any 1836 Technologies asset as needed.

4.2 Access to Web Site Monitoring Reports

Authorized ITS members, Incident Response Team members, and the Legal Department will have access to all reports and data if necessary in order to respond to a security incident. Internet Use reports that identify specific users, sites, teams, or devices will only be made available to personnel outside ITS upon written or e-mail request from an authorized Human Resources Representative.

4.3 Internet Use Filtering System

4.3.1 1836 Technologies Personnel shall not access, transmit, upload, download, print, display or otherwise disseminate the following types of material while on the 1836 Technologies Network or while using 1836 Technologies assets:

- Adult/sexually explicit and/or obscene images, data, or other material;
- Tasteless, Defamatory, and/or Offensive Content;
- Racially offensive;

- Fraudulent or Otherwise unlawful; and/or;
- Promotes violence, Intolerance and/or Hatred;
- Any data capable of being transformed into obscene or indecent images or material

This includes obscene language, pornography, hostile material relating to gender, sex, race, sexual orientation, religious, political convictions, disability or information that would cause or promote incitement of hatred, violence or any other intimidating material that is designed or could be used to cause offence, annoyance, inconvenience, needless anxiety or which would contravene any Trust policy, in particular equal opportunities or harassment, or break any law.

4.3.2 1836 Technologies Personnel cannot:

i. Intentionally circumvent security mechanisms such as cracking passwords, exploiting system vulnerabilities, or using systems in excess of granted privileges;

ii. Intentionally write, compile, copy, propagate, execute, or attempt to introduce any malicious computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer system. Such software may be referred to as malware virus, bacteria, worm, or a Trojan Horse; and

iii. Transmit, upload, post or discuss Personal Identifiable Information (PII), Protected Health Information (PHI), or sensitive Government or 1836 Technologies company data with any third party without prior written authorization; or

4.3.3 In addition to the above, the Internet may not be accessed and used for any of the following:

- Any activity that infringes copyright
- Transmission of unsolicited commercial or advertising material
- Deliberate unauthorized access to facilities or services accessible via the Internet
- Corrupting or destroying another user's data
- Any activity that would violate the privacy of others
- Any activity that would risk bringing the organization into disrepute or place the Trust in a position of liability
- Cause damage or disruption to organizational systems
- Any activity that would violate the laws and regulations of the European Union
- Not to be used for any secondary paid employment or voluntary services
- Not to be used to run a personal business

4.3.4 The IT Department reserves the right to block access to Internet websites and protocols that are deemed inappropriate for 1836 Technologies's corporate environment. The following protocols and categories of websites are examples of the type of websites that may be blocked:

- Adult/Sexually Explicit Material
- Advertisements & Pop-Ups
- Gambling
- Hacking
- Illegal Drugs
- Intimate Apparel and Swimwear
- Peer to Peer File Sharing
- SPAM, Phishing and Fraud
- Spyware
- Tasteless Defamatory, and/or Offensive Content
- Racially offensive, promoting violence, Intolerance and/or Hatred

4.4 Internet Use Filtering Exceptions

If a site is blocked, then 1836 Technologies Personnel may only access that blocked site with prior written permission if appropriate and necessary for business purposes. If any Personnel need access to a site that is blocked and appropriately categorized, they must submit a request to their appraisal manager. They will then present all approved exception requests to ITS in writing or by email, and ITS will evaluate the request and consider unblocking that site or category.

5.0 Enforcement

5.1 1836 Technologies personnel are expected to report suspected violations of this policy to the Legal Department.

5.2 Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Special Approval for European Union (EU) Users

Due to privacy concerns within the EU, special approvals and consents from the 1836 Technologies Personnel must be undertaken before a deep packet inspection is started. 1836 Technologies ITS will first ask the affected 1836 Technologies Personnel permission to conduct a further analysis of their packet payloads to determine the cause of the alert. The user will then be informed of their options, and if they agree to the inspection, they will be required to complete the attached EU Consent Form. If the user consents to ITS inspecting the packet payload, ITS will then examine the packets captured. If the user denies ITS' request, the user may be disconnected from the 1836 Technologies Network if it is determined that his/her computer will continue to pose a risk to the 1836 Technologies Network.

7.0 Definitions

Hacking Sites - Sites that provide content about breaking or subverting computer security controls.

Incident - A reported security event or group of events that has proven to be a verified information technology security breach. An incident may also be an identified violation or imminent threat of violation of information technology security policies, or a threat to the security of system assets. Some examples of possible information technology security incidents are, but are not limited to:

- Loss of confidentiality of information
- Compromise of integrity of information
- Loss of system availability
- Denial of service
- Misuse of service systems or information

Internet - an unclassified electronic communications network that connects computer networks and organizational computer facilities around the world.

Internet Filtering – Using technology that monitors each instance of communication between devices on the corporate network and the Internet and blocks traffic that matches specific rules.

Intrusion detection - The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

IP Address – Unique network address assigned to each device to allow it to communicate with other devices on the network or Internet.

Peer to Peer File Sharing – Services or protocols such as BitTorrent and Kazaa that allow Internet connected hosts to make files available to or download files from other hosts. Social Networking Services – Internet sites such as Myspace and Facebook that allow users to post content, chat, and interact in online communities.

Phishing – attempting to fraudulently acquire sensitive information by masquerading as a trusted entity in an electronic communication.

SMTP – Simple Mail Transfer Protocol. The Internet Protocol that facilitates the exchange of mail messages between Internet mail servers.

SPAM – Unsolicited Internet Email.

User ID – User Name or other identifier used when an associate logs into the corporate network.

8.0 Revision History

__/2010 – Draft Completed, _________________

DRAFT – PRIVILEGED & CONFIDENTIAL

DRAFT EU Consent Form

I, _____________________, having been informed of my right not to have a search made of the computer systems hereinafter mentioned without a search warrant and of my right to refuse consent to such a search, hereby authorize 1836 Technologies International, Inc., Information Technology Services, to conduct a complete search of the computer system : ______(insert host name of the computer here)______ and its communications used to conduct 1836 Technologies business. This search includes the deep packet inspection of all communications between the aforementioned computer and the internet in an effort to safeguard the 1836 Technologies network from malicious activities.

You are hereby authorized by me to take from this location any property which you need to complete your analysis, assessment, and/or resolution of a possible privacy or internet security incident. This written permission is being given by me voluntarily and without threats or promises of any kind. I have not been threatened, placed under duress or promised anything in exchange for my consent. I have read and understand this form. I understand the English language and have been able to communicate with the 1836 Technologies ITS representatives regarding the possible privacy and/or IT security incident.

I understand that I this consent only applies to this incident and that my further consent will be required for any future incidents that may occur.

Dated, signed and witnessed

Signed:____________________________

Date: ____________________________

Witnessed: _________________________

1836 Technologies International Work Plan

1836 Technologies, Inc. (1836 Technologies), as a government contractor, is required to comply with laws, regulations, standards, directives and instructions pertaining to information security. The Federal Information Security Management Act (FISMA) requires 1836 Technologies to implement an information security program to operate or use Federal Information Systems. This program requires adherence to standards developed by the National Institute of Standards and Technology (NIST). As a contractor with the Department of Defense (DoD), 1836 Technologies is also required to comply with Directives and Instructions of the DoD pertaining to Information Assurance (IA) when such systems are National Security Systems. To prepare and implement an enterprise-wide information security program, 1836 Technologies will be required to include and harmonize the FISMA and the DoD IA requirements. In an effort to attain this goal, this proposed work plan has been prepared for 1836 Technologies to identify the tasks and estimate the budget for the following tasks:

Task 1. Prepare Basic Policies and Procedures;
Task 2. Crosswalk of Information Security Requirements; and
Task 3. Conduct Administrative Risk Assessment.

This work plan describes each of these tasks followed by an estimated completion schedule and budget. The tasks may change based on our review of the existing 1836 Technologies security program, policies, procedures and organizational structure. Our goal is to incorporate and utilize as much of 1836 Technologies's existing information security program as possible in the new enterprise-wide information security program.

Task 1. Prepare Basic Policies and Procedures

The purpose of this first task is to provide the basic policies and procedures that provide the necessary building blocks for an enterprise-wide information security program. Bringing 1836 Technologies into compliance with FISMA and DoD Information Assurance (IA) requirements will require more than policy and procedure implementation. However, the basic policies and procedures are required for compliance with FISMA and DoD IA requirements and represent best industry practices in information security.

The full list of 29 basic policies and procedures and their descriptions, as previously provided, is included in Attachment A for your convenience. The following is a summarized list of all policies and procedures, which should be developed by 1836 Technologies:

1. Corporate Policy (1836 Technologies: Enterprise Security Policy)
2. Information and Technology Risk Management Policy
3. Roles and Responsibilities
4. Acceptable Use Policy (1836 Technologies: System Rules of Behavior)

5. Data Classification Policy
6. Data Handling Policy
7. Access Controls
8. Password Policy
9. Third- Party Access
10. Incident Response Policy (1836 Technologies: Incident Response Plan, Forensic Procedures/Cyber Investigations, Responding to Government Investigations Regarding Security Instance and Loss or Potential Loss of PII)
11. Asset Management Policy (Use of Non-1836 Technologies Owned Equipment)
12. Systems and Application Monitoring and Logging (1836 Technologies): Internet/Network Usage and Monitoring Policy (US and Europe))
13. Configuration Management Policy
14. Change Management Policy
15. Physical and Environmental Protection Policy
16. Security Planning Process (1836 Technologies: System Security Plan)
17. Systems and Services Development, Acquisition and Life Cycle
18. System and Communication Detection Policy
19. System and Information Integrity
20. Information System Maintenance
21. Encryption Policy (1836 Technologies: Encryption Policy)
22. Certification Accreditation/Security Assessments Policy
23. Security Awareness and Training Policy
24. Human Resources Security (1836 Technologies: 1836 Technologies Employee Handbook Revisions)
25. Media Handling, Including Management and Disposal (1836 Technologies: Assessment, review, and updating of policies and procedures for disposal of confidential information, corporate assets, and PII data)
26. Records Management and Retention Program
27. Data Back-Up
28. Disaster Recovery and Business Continuity (IT Contingency Plan (ITCP))
29. Data Protection and Privacy of Personal Information (1836 Technologies policy re PII including Definition of PII)

Crosswalk of Information Security Requirements

In this task, for each of the policies and procedures created by 1836 Technologies, we will identify those sections of FISMA (including NIST standards) and DoD IA requirements that apply. The references to the laws, regulations, directives, instructions and standards, as applicable, will be included in each policy and procedure to demonstrate due diligence performed by 1836 Technologies in its compliance efforts.

Perform Administrative Security Assessment

In this task, 1836 Technologies must assess its management of cyber security against NIST standards and DoD IA requirements This review will confirm that the policies and procedures comply with FISMA and DoD IA requirements and also reflect actual operations. The three areas that will be reviewed in this administrative risk assessment are Cyber Security Infrastructure, Security of Third-Party Access, and Personnel Security, described as follows:

Cyber Security Infrastructure.   Need to assess 1836 Technologies's information security infrastructure in order to draft appropriate policies and procedures:

- Cyber security governance and infrastructure. This includes a review of how information security is organized within 1836 Technologies and whether proper resources are applied to manage administrative security requirements.
- Management of information security. This includes a review of whether 1836 Technologies management actively supports security within 1836 Technologies through clear direction, demonstrated commitment, and explicit assignment and acknowledgment of information security responsibilities.
- Information security coordination. This part of the review focuses on how security activities are coordinated by representatives from different parts of 1836 Technologies with relevant roles and job functions.
- Allocation of information security responsibilities. The identification and communication of security roles and responsibilities are reviewed to determine whether they are clearly defined.
- Specialist information security advice. Assess the proper use of specialized information security advice by 1836 Technologies, including utilizing internal specialized information security resources.
- Agreements to protect 1836 Technologies assets and the information that they store, process and transmit. Review nondisclosure and acceptable use agreements to determine whether 1836 Technologies's needs for protection of information and assets are identified and regularly reviewed.
- Independent review of information security. We will determine the use and frequency of the use of independent audits and assessments.

Security of Third Party Access. Assess how contractors and other third parties handle information security requirements, looking at the following:

- Identification of risks from third party access. Assess potential risks involving external parties and safeguards that have been implemented to manage the risks.
- Security requirements in third party contracts. Contracts with third parties that access, process, communicate or manage 1836 Technologies's information or information processing systems need to be reviewed to determine if they cover relevant security requirements.

Personnel Security.

- Security in job definition and contractor selection. Assess whether security roles and responsibilities of employees, contractors and third-parties are defined and documented in accordance with the 1836 Technologies's information security policy
- Personnel screening. The use of background verification checks on candidates for employment, contractors and third parties need to be reviewed to determine whether the practices are carried out in accordance with relevant laws and regulations.
- Terms and conditions of employment. Assess whether 1836 Technologies requires employees, contractors and third parties to agree to adhere to 1836 Technologies policies and procedures regarding information security.
- Training and awareness. Need tol review training and awareness programs to determine whether 1836 Technologies requires employees, contractors and third parties to receive appropriate awareness training in cyber security policies and procedures.
- Responding to Security Incidents. Assess how security incidents are handled at 1836 Technologies including the reporting of security incidents, security weaknesses and software malfunctions, learning from incidents and disciplinary process.

The information gathered from this task will be used to determine if current 1836 Technologies practices comply with relevant NIST guidelines and DoD IA requirements. Policies and procedures will need to be finalized so as to reflect current practices before the policies and procedures are finalized and implemented. By incorporating this risk assessment into the policy and procedure development, 1836 Technologies will demonstrate that it is following industry best practices to comply with federal guidelines requiring organizations to ensure that their policies and procedures reflect actual operations.

Attachment A

Basic Policies and Procedures for an
Enterprise-Wide Information Security Program

POLICY AND PROCEDURE	PURPOSE	DoD IA	FISMA/FIPS /NIST	1836 Technologies STATUS
Corporate Policy	Provides management direction and support for information security in accordance with business requirements and relevant laws and regulations.	✓	✓	
Information and Technology Risk Management Policy	Promotes the systematic application of policies, procedures and practices to managing information and technology risks.	✓	✓	
Roles and Responsibilities	Provides a management framework to initiate and manage information security within 1836 Technologies. Identifies governance and key roles and responsibilities for implementation and maintenance of the information security program.	✓	✓	
Acceptable Use Policy	Outlines the acceptable use of information technology equipment at 1836 Technologies, includes basic overview of requirements to protect the system from unauthorized access, protection from malicious code and password management. (This is often signed by employees after they attend awareness training.)	✓	✓	
Data Classification Policy	Ensures that the information assets are classified so that they receive appropriate levels of protection.	✓	✓	
Data Handling Policy	Covers managing risks to the confidentiality, integrity and availability of 1836 Technologies information.	✓	✓	
Access Controls	Ensures that access to electronic information is granted and authorized appropriately.	✓	✓	

POLICY AND PROCEDURE	PURPOSE	DoD IA	FISMA/FIPS /NIST	1836 Technologies STATUS
Password Policy	Provides instructions on properly establishing using and maintaining passwords.	✓	✓	
Third Party Access	Provides safeguards for management of third-party network connections.	✓	✓	
Incident Response Policy	Sets forth procedures for preparation, detection and response (investigation, and analysis, mitigation, notice) to a security incident.	✓	✓	
Asset Management Policy	Covers management of risk for IT equipment and applications owned, licensed or controlled by 1836 Technologies.	✓	✓	
System and Application Monitoring and Logging	Includes high-level requirements for logging and reviewing activities on systems and applications.	✓	✓	
Configuration Management Policy	Requires mandatory baseline configuration settings to be established for information systems connected to 1836 Technologies trusted networks.	✓	✓	
Change Management Policy	This policy includes a process for managing changes to ensure that only documented and authorize changes are applied.	✓	✓	
Physical and Environmental Protection Policy	Ensures that 1836 Technologies information system assets are sufficiently protected from physical and environmental threats to prevent the loss, damage, or compromise of assets, an interruption to business activities.	✓	✓	
Security Planning Process	Provides an overview of the security requirements for information systems and describes the security controls in place or planned for meeting those requirements.	✓	✓	
Systems and Services Development, Acquisition and Life Cycle	Provides for formal enterprise development procurement and contracting processes when developing or acquiring hardware, applications, and software and associated services. This includes ensuring proper security throughout the	✓	✓	

POLICY AND PROCEDURE	PURPOSE	DoD IA	FISMA/FIPS /NIST	1836 Technologies STATUS
	Systems Development life Cycle (SLDC).			
System and Communication Protection Policy	Requires the establishment of mandatory security controls to manage information systems communications with 1836 Technologies trusted networks.	✓	✓	
System and Information Integrity	Provides for adequate technical and procedural controls to be employed and maintained on critical information systems to ensure system and information integrity.	✓	✓	
Information System Maintenance	Sets forth procedures for managing information systems updates, including roles, responsibilities and the tools used to perform system maintenance.	✓	✓	
Encryption Policy	Procedures for implementing and using encryption.	✓	✓	
Certification, Accreditation/Security Assessments Policy	Establishes requirements for the certification and accreditation processes for information systems and applications.	✓	✓	
Security Awareness and Training Policy	Establishes training on information security for 1836 Technologies employees that is commensurate with their job responsibilities.	✓	✓	
Human Resources Security	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of unauthorized access, theft, fraud or misuse of facilities.	✓	✓	
Media Handling, Including Data Management, and Disposal	Procedures for handling of media to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.	✓	✓	
Records Management and Retention Program	To protected important records from loss, destruction, and falsification, in accordance with	✓	✓	

POLICY AND PROCEDURE	PURPOSE	DoD IA	FISMA/FIPS /NIST	1836 Technologies STATUS
	statutory, regulatory, contractual, and business requirements.			
Data Backup	Procedures for regular backups of IT Systems and data contained on them. This include secure storage, and the ability to recover data from backups when needed.	✓	✓	
Disaster Recovery and Business Continuity	A managed process for disaster recovery and business continuity throughout the organization.	✓	✓	
Data protection and privacy of personal information	A policy to protect personally identifiable information as required in relevant laws regulations and contractual requirements.	✓	✓	

Privacy Incidents:

A Privacy Incident is any potential or actual compromise of *personally identifiable information (PII)* in a form that could be accessed by an unauthorized person. The Government has characterized privacy incidents to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

Examples of privacy incidents include:

- Hacker obtains information from 1836 Technologies laptops which includes Name, SSN, Date of Birth
- Lost or stolen thumb drive or portable hard drive of PII
- Shipper loses a package of employee applications
- Unauthorized access to personnel files
- File left on community printer with names, addresses and account numbers
- A file folder containing prospective employee resumes is missing
- Employee roster posted on 1836 Technologies portal, disclosing name, personal cell phone number, and home address
- E-mail containing salaries and raises transmitted from a 1836 Technologies e-mail account to a personal e-mail account
- Key logger gains access to a computer and its accounts

Note: 1836 Technologies personnel should identify whether the PII involved in the incident originated from 1836 Technologies or from a client. Continue normally through this guide if the information originated from 1836 Technologies. If the information originated from a client, notify the Privacy Division immediately for coordination and action with the client privacy personnel. This process will occur concurrently to 1836 Technologies privacy incident response. DO NOT CONTACT THE CLIENT DIRECTLY.

This is the information we would want to capture on an Initial Privacy Incident Report:

The Initial Privacy Incident Report is used to report information initially gathered about a Privacy Incident. This form is found on the **1836 Technologies Privacy Incident Reporting Portal**. Examples of information gathered in this report include:

- Name, Employee ID#, 1836 Technologies phone number, and 1836 Technologies email address of the 1836 Technologies personnel who discovered the incident (if they are willing to provide this information);
- Date and time of the incident; and

- A general description of the incident and the PII that is involved (i.e., the category of PII that was compromised, but not the actual PII in the report).

> ***Important:*** *Do not report the actual PII from the initial incident, because by doing so you will create another Privacy Incident.*

- To whom it was disclosed, to the extent known;
- The risk of the PII being misused expressed in terms of impact and likelihood;
- Security controls known to protect the information (e.g., password-protection, encryption);
- Steps that have already been taken to reduce the risk of harm; and
- Any additional steps that may be taken to mitigate the situation.

- **Is the incident suspected or confirmed? ***
- **Date Incident Occurred**
- **Date Incident Detected ***
- **Location Incident Occurred**
- **Does the incident involve Paper, Electronic Records, or both? ***
- **Electronic Record Type(s), if applicable (Choose all that apply):**
  - CD/DVD
  - Desktop computer
  - Lap top computer
  - e-mail
  - electronic file (other than e-mail)
  - External hard drive
  - Flash drive/thumb drive/USB key
  - Other: ____________________

Paper Record Type(s), if applicable (Choose all that apply):

- Fax
- Mailing
- Printer/Scanner
- Other: _________

Was personally identifiable information involved in the incident? *

Yes
No

Was personally identifiable information exposed?

Yes
No

If yes, how was the personally identifiable information exposed?

Identify the type(s) of personally identifiable information (but not the actual information disclosed or lost):

- Name
- Date of Birth
- Mailing Address
- Telephone Number
- Social Security Number
- E-mail Address
- ZIP Code
- Financial Account Number
- Certificate/License Number
- Vehicle Identifiers
- Immigration Identification Numbers
- Biometric Identifiers
- IP Addresses/URLs
- Health or Medical Information
- Driver's License/Passport/State ID Number
- Employee Identification Number

- What type of information was compromised?

  - 1836 Technologies Internal Data
  - Client Data
  - Other

If Client Data, what Client and/or what contract?

Was the information password protected?

- Yes
- No
- Unknown

Was the information encrypted?

- Yes
- No
- Unknown

Describe the physical security measures:

Number of records affected (approximate if unsure)

Number of individuals affected (approximate if unsure)

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

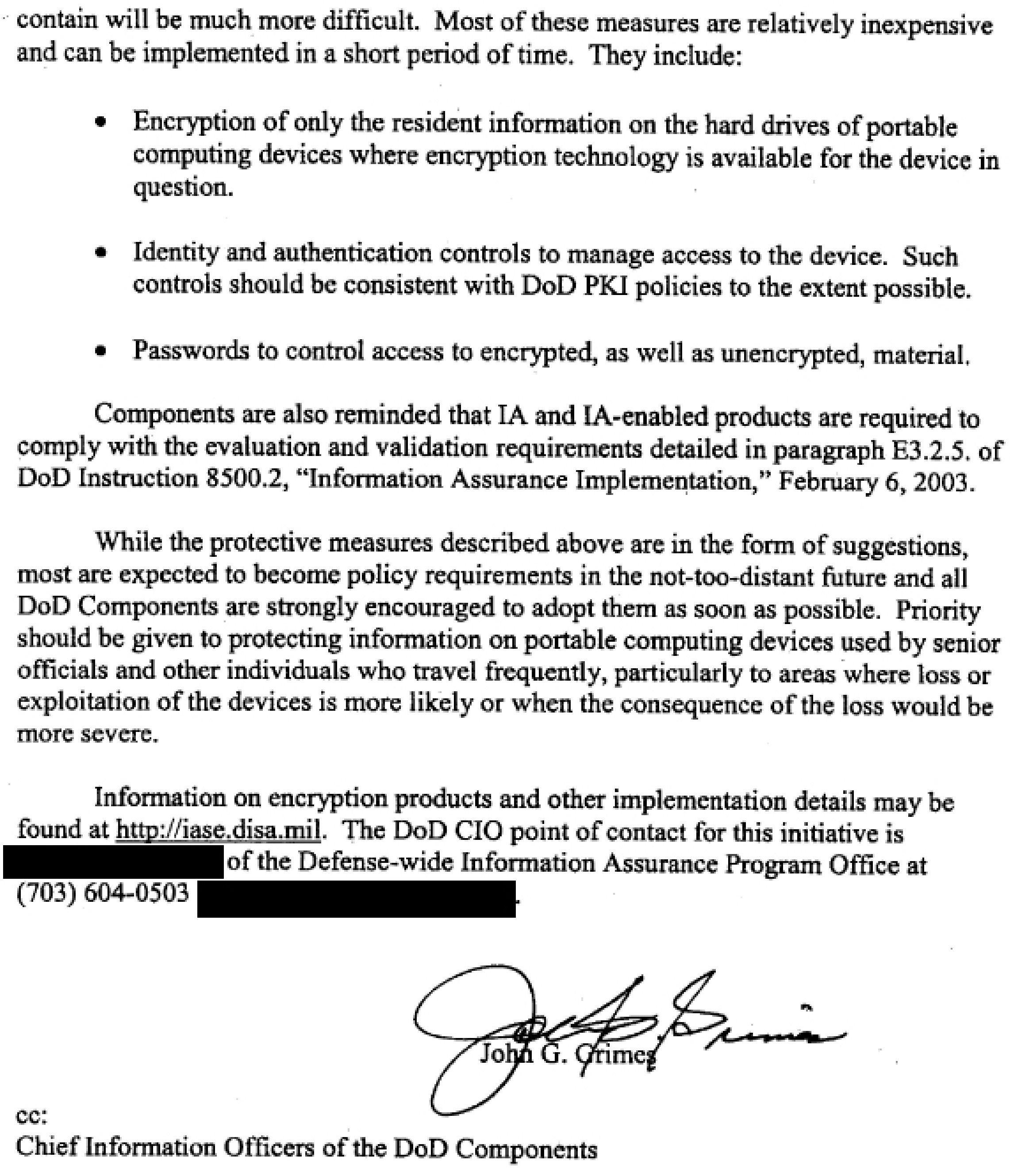
APR 18 2006

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMBATANT COMMANDERS
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Protection of Sensitive Department of Defense (DoD) Data at Rest On Portable Computing Devices

The proliferation of portable computing devices across the DoD requires a fresh look at current policies governing the protection of sensitive data at rest. Recent advances in computing technology have resulted in greatly increased computing power and storage capacity for portable computing devices. These advances have enhanced both effectiveness and efficiency by allowing DoD personnel to perform their duties at home or while on official travel, but they are not without costs. Along with the increased computing capability and portability there are also more and greater threats to the unclassified sensitive DoD information that is likely to be resident on the hard drives of the devices. Portable computing devices are much more likely to be lost, stolen, or exploited while unattended than are those that permanently remain in office spaces.

This memorandum provides suggestions on technical means to protect unclassified sensitive information on portable computing devices used within DoD. The measures are in addition to the normal physical security required for such devices so that, if they fall into the wrong hands for any reason, access to the sensitive DoD information they



contain will be much more difficult. Most of these measures are relatively inexpensive and can be implemented in a short period of time. They include:

- Encryption of only the resident information on the hard drives of portable computing devices where encryption technology is available for the device in question.

- Identity and authentication controls to manage access to the device. Such controls should be consistent with DoD PKI policies to the extent possible.

- Passwords to control access to encrypted, as well as unencrypted, material.

Components are also reminded that IA and IA-enabled products are required to comply with the evaluation and validation requirements detailed in paragraph E3.2.5. of DoD Instruction 8500.2, "Information Assurance Implementation," February 6, 2003.

While the protective measures described above are in the form of suggestions, most are expected to become policy requirements in the not-too-distant future and all DoD Components are strongly encouraged to adopt them as soon as possible. Priority should be given to protecting information on portable computing devices used by senior officials and other individuals who travel frequently, particularly to areas where loss or exploitation of the devices is more likely or when the consequence of the loss would be more severe.

Information on encryption products and other implementation details may be found at http://iase.disa.mil. The DoD CIO point of contact for this initiative is [redacted] of the Defense-wide Information Assurance Program Office at (703) 604-0503 [redacted].

John G. Grimes

cc:
Chief Information Officers of the DoD Components

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

AUG 18 2006

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
COMBATANT COMMANDERS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, PROGRAM ANALYSIS AND EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)

References: (a) OMB M-06-16, "Protection of Sensitive Agency Information," 23 June 2006

(b) OMB M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006.

(c) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

This memorandum establishes guidance for the protection of Personally Identifiable Information (PII) in accordance with references (a) and (b).

DoD Components are directed to ensure that all PII not explicitly cleared for public release is protected according to Confidentiality Level Sensitive, as established in reference (c). Additionally, all DoD information and data owners shall conduct risk assessments of compilations of PII and identify those needing more stringent protection for remote access or mobile computing. The attachment provides detailed implementation guidance.

The points of contact for this memorandum are Donald Jones (703) 614-6640, donald.jones@osd.mil and Gus Guissanie (703) 614-6132, gary.guissanie@osd.mil.

Priscilla E. Guthrie
Principal Deputy
(DoD CIO)

Attachment:
Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)

Department of Defense Guidance on Protecting Personally Identifiable Information (PII)

August 18, 2006

Subject: Department of Defense Guidance on Protecting Personally Identifiable Information (PII)

References: (a) OMB M-06-16, "Protection of Sensitive Agency Information," 23 June 2006

(b) OMB M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," July 12, 2006.

(c) DoDD 5400.11, "DoD Privacy Program," Nov 16, 2004.

(d) DoDD 8000.1, "Management of DoD Information Resources and Information Technology," change 1 March 20, 2002

(e) through (h), see enclosure 1.

1. PURPOSE.

This implements DoD policy regarding the protection of personally identifiable information as established in references (a-c) and according to references (d-h).

2. APPLICABILITY AND SCOPE.

This policy applies to

2.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff (CJCS), the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Component(s)").

2.2. All DoD-owned or controlled information systems or services that receive, process, store, display or transmit DoD information regardless of classification or sensitivity. This includes but is not limited to information systems or services that contain information meeting the criteria for designation as Privacy Act records as defined in reference (c). As established in reference (e) and related issuances, this also includes contracted or outsourced access to DoD information and resources.

3. DEFINITIONS are at enclosure 2.

4. POLICY.

It is DoD policy that:

4.1. All PII shall be evaluated for impact of loss or unauthorized disclosure and protected accordingly.

4.2. All PII electronic records shall be assigned a High or Moderate PII Impact Category according to the definitions established in this policy and protected at a Confidentiality Level of Sensitive or higher as established in reference (e)[1], unless specifically cleared for public release (e.g., the name and contact information for selected public officials). Further, electronic PII records assigned a High Impact Category shall be protected as follows:

4.2.1. Such records shall not be routinely processed or stored on mobile computing devices or removable electronic media without express approval of the Designated Accrediting Authority (DAA) (previously Designated Approving Authority). See reference (f).

4.2.2. Except for compelling operational needs, any mobile computing device or removable electronic media that processes or stores High Impact electronic records shall be restricted to workplaces that minimally satisfy Physical and Environmental Controls for Confidentiality Level Sensitive as established in reference (e) (hereinafter referred to as "protected workplaces").

4.2.3. Any mobile computing device containing High Impact electronic records removed from protected workplaces, including those approved for routine processing, shall:

4.2.3.1. Be signed in and out with a supervising official designated in writing by the organization security official.

4.2.3.2. Require certificate based authentication using a DoD or DoD-approved PKI certificate on an approved hardware token to access the device.

[1] Any Mission Assurance Category is acceptable for DoD information systems processing PII.

4.2.3.3. Implement IA Control PESL-1 (Screen Lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended).

4.2.3.4. Encrypt all data at rest, i.e., all hard drives or other storage media within the device as well as all removable media created by or written from the device while outside a protected workplace. Minimally, the cryptography shall be NIST-certified (i.e., FIPS 140-2 or current). See Reference (e), ECCR (Encryption for Confidentiality (Data at Rest)). Information on encryption products and other implementation details can be found at http://iase.disa.mil.

4.2.4. Only DoD authorized devices shall be used for remote access. Any remote access, whether for user or privileged functions, must conform to both IA Control EBRU-1 (Remote Access for User Functions) and EBRP-1 (Remote Access for Privileged Functions) as established in reference (e).

4.2.5. Remote access to High Impact PII electronic records is discouraged, is permitted only for compelling operational needs, and:

4.2.5.1. Shall employ certificate based authentication using a DoD or DoD-approved PKI certificate on an approved hardware token.

4.2.5.2. The remote device gaining access shall conform to IA Control PESL-1 (Screen Lock), with a specified period of inactivity not to exceed 30 minutes (15 minutes or less recommended). See reference (e).

4.2.5.3. The remote device gaining access shall conform to IA Control ECRC-1, Resource Control. See Reference (e).

4.2.5.4. Download and local/remote storage of PII records is prohibited unless expressly approved by the DAA.

4.2.6. Any High Impact electronic PII records stored on removable electronic media taken outside protected workplaces shall signed in and out with a supervising official and shall be encrypted. Minimally, the cryptography shall be NIST-certified. See Reference (e), ECCR (Encryption for Confidentiality (Data at Rest)).

4.3. Loss or suspected loss of PII shall be reported to:

4.3.1. The United States Computer Emergency Readiness Team (US CERT) within one hour in accordance with the requirements of reference (b) and guidance at www.us-cert.gov, as published.

4.3.2. The DoD Component Privacy Office/Point of Contact (POC) within 24 hours and the DoD Privacy Office within 48 hours or as established by the Defense Senior Privacy Official (paragraph 5.2).

4.4. The underlying incident that led to the loss or suspected loss of PII (e.g., computer incident, theft, loss of material, etc.,) shall continue to be reported in accordance with established procedures (e.g., to designated Computer Network Defense (CND) Service Provider according to reference (g); law enforcement, chain of command, etc.).

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer shall address the protection of PII in the management DoD information resources and information technology consistent with reference (d).

5.2. The Director for Administration and Management (DA&M), as the Senior Privacy Official for the Department of Defense shall establish procedures for reporting the loss or suspected loss of PII within the Department of Defense and ensure that incidents involving the loss of PII are addressed consistent with the requirements of reference (c).

5.3. Heads of DoD Components shall:

5.3.1. In accordance with this policy and direction from the DoD Senior Privacy Official, establish reporting procedures to ensure that loss or suspected loss is reported in accordance with paragraphs 4.3 and 4.4 above.

5.3.2 Ensure Information Owners or Data Owners identify PII, evaluate the risk of loss or unauthorized disclosure, assign Impact Categories for electronic PII records, and establish appropriate protection measures for PII in other media.

5.3.3 Ensure Information Assurance Managers in concert with other certification and accreditation team members incorporate protection measures for High Impact electronic PII records into the DoD IA certification and accreditation process as defined in reference (f).

5 3.4. Ensure supervising officials establish logging and tracking procedures for High Impact electronic PII records on mobile computing devices or portable media removed from protected workplaces.

6. PROCEDURES are as specified above and in references (e-h).

7. EFFECTIVE DATE.

This policy is effective immediately.

Enclosures – 3
E1. References, continued
E2. Definitions
E3. Traceability to OMB Checklist

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003

(f) DoD CIO Memorandum, “Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process Guidance,” July 6, 2006

(g) CJCSM 6510.01, “Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND), Change 3, March 8 2006

(h) DoD CIO Memorandum, "Department of Defense (DoD) Privacy Impact Assessment (PIA) Guidance", 28 October 2005

E2. ENCLOSURE 2.

DEFINITIONS

E2.1. Individual. A living person who is a citizen of the United States or an alien lawfully admitted for permanent residence. The parent of a minor or the legal guardian of any individual also may act on behalf of an individual. Members of the United States Armed Forces are "individuals." Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities are not "individuals." Reference (c).

E2.2. Individual Identifier. Information associated with a single individual and used to distinguish him or her from other individuals, e.g., name, social security number or other identifying number, symbol, or other identifying particular such as a finger or voice print or photograph.

E2.3. Personally Identifiable Information (PII). Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. Reference (b).

E2.4. PII Impact Category. For DoD information assurance purposes, consistent with reference (a) and FIPS 199, electronic PII records are categorized according to the potential negative impact of loss or unauthorized disclosure:

E2.4.1. High Impact. Any Defense-wide, organizational (e.g., unit or office), or program or project level compilation of electronic records containing PII on 500 or more individuals stored on a single device or accessible through a single application or service, whether or not the compilation is subject to the Privacy Act. Also, any compilation of electronic records containing PII on less than 500 individuals identified by the Information or Data Owner as requiring additional protection measures. Examples: A single mobile computing or storage device containing PII on 500 or more individuals, even if the PII is distributed across multiple files or directories, is considered High Impact PII. A DoD enclave of 500 or more users, with the PII for each user embedded in his/her individual workstation, is not considered High Impact PII.

E2.4.2. Moderate Impact. Any electronic records containing PII not identified as High Impact.

E2.5. PII Electronic Record. Any item, collection, or grouping of information in electronic form maintained by a DoD Component that associates personal information such as education, financial transactions, medical history, criminal or employment history, with an individual identifier. Also any item, collection, or grouping of information in electronic form that associates two or more individual identifiers, e.g., name and social security number. Electronic records that contain information about education, financial transactions, medical history, or criminal or employment history but do not include individual identifiers are not considered PII electronic records.

E2.6. Remote Access. Enclave-level access for authorized users external to the enclave that is established through a controlled access point (e.g., a remote access server or communications server) at the enclave boundary. Reference (e) modified to include controlled access point examples.

E1. ENCLOSURE 3.

TRACEABILITY TO OMB CHECKLIST

Checklist Item (Reference(a))	DoD Guidance / Methodology	Remarks
Step 1. Confirm the identification of personally identifiable information protection needs.	1. Conduct Privacy Impact Assessments as required by DoD policy, (reference (h)), http://www.dod.mil/nii/pia/	Equivalent to or exceeds PL-5 and associated NIST SP 800-53 controls
	2. Assign DoD Mission Assurance Category (MAC) and Confidentiality Level according to DoDI 8500.2 and review associated IA Controls. Ensure that the minimum Confidentiality Level for any DoD information system processing PII is Sensitive.	Equivalent to or exceeds RA-2 and associated NIST SP 800-53 controls
	3. Identify PII and assign PII Impact Category according to this policy.	Equivalent to or exceeds RA-4 and associated NIST SP 800-53 controls
Step 2. Verify adequacy of organizational policy.		The formulation of this policy was based upon a review of all SP 800-53 controls identified for consideration in the OMB checklist and all DoDI 8500.2 IA Controls, including those mapped in Appendix G to the SP 800-53 controls identified for consideration in the OMB checklist. This policy verifies and updates DoD policy, thus satisfying Step 2 for all DoD information systems and services.

Checklist Item (Reference(a))	DoD Guidance / Methodology	Remarks
Step 3. Implement protections for PII being transported and/or stored offsite. Step 4. Implement protections for remote access to PII.	For Moderate Impact PII, implement the IA Controls assigned according to reference (e). For High Impact PII, incorporate the PII protection measures identified in this policy into assigned IA Controls and C&A activities (e.g., IA Controls Implementation Plan, POAM). Note the PII measures in this policy specifically address PII being transported and/or stored off site and remote access.	Steps 3 and 4 are satisfied as each DoD information system manages compliance with its assigned IA Controls and the measures established in this issuance, if required.

Department of Defense
DIRECTIVE

NUMBER 8500.*0*1*E*
October 24, 2002
Certified Current as of April 23, 2007

ASD(NII)/DoD CIO

SUBJECT: Information Assurance (IA)

References: (a) Section 2224 of title 10, United States Code, "Defense Information Assurance Program"
(b) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988 (hereby canceled)
(c) DoD 5200.28-M, "ADP Security Manual," January 1973 (hereby canceled)
(d) DoD 5200.28-STD, "DoD Trusted Computer Security Evaluation Criteria," December 1985 (hereby canceled)
(e) through (a*h*), see enclosure 1

1. PURPOSE

This Directive:

1.1. Establishes policy and assigns responsibilities under reference (a) to achieve Department of Defense (DoD) information assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare.

1.2. Supersedes DoD Directive 5200.28, DoD 5200.28-M, DoD 5200.28-STD, and DoD Chief Information Officer (CIO) Memorandum 6-8510 (references (b), (c), (d), and (e)).

1.3. Designates the Secretary of the Army as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

1.4. Authorizes the publication of DoD 8500.1-M consistent with DoD 5025.1-M (reference (f)).

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as "the DoD Components").

2.1.2. All DoD-owned or -controlled information systems that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity, including but not limited to:

2.1.2.1. DoD information systems that support special environments, e.g., Special Access Programs (SAP) and Special Access Requirements (SAR), as supplemented by the special needs of the program.

2.1.2.2. Platform IT interconnections, e.g., weapons systems, sensors, medical technologies or utility distribution systems, to external networks.

2.1.2.3. Information systems under contract to the Department of Defense.

2.1.2.4. Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.

2.1.2.5. Information systems of Nonappropriated Fund Instrumentalities.

2.1.2.6. Stand-alone information systems.

2.1.2.7. Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.

2.2. Nothing in this policy shall alter or supercede the existing authorities and policies of the Director of Central Intelligence (DCI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 (reference (g)) and other laws and regulations.

2.3. This policy does not apply to weapons systems as defined by DoD Directive *5144.1* (reference (h)) or other IT components, both hardware and software, that are physically part of, dedicated to, or essential in real time to a platform's mission performance where there is no platform IT interconnection.

3. DEFINITIONS

Terms used in this Directive are defined in National Security Telecommunications and Information Systems Security Instruction Number 4009 (reference (i)) or enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Information assurance requirements shall be identified and included in the design, acquisition, installation, operation, upgrade, or replacement of all DoD information systems in accordance with 10 U.S.C. Section 2224, Office of Management and Budget Circular A-130, Appendix III, DoD Directive 5000.1 (references (a), (j), and (k)), this Directive, and other IA-related DoD guidance, as issued.

4.2. All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness. For IA purposes all DoD information systems shall be organized and managed in the four categories defined in enclosure 2: automated information system (AIS) applications, enclaves (which include networks), outsourced IT-based processes, and platform IT interconnections.

4.3. Information assurance shall be a visible element of all investment portfolios incorporating DoD-owned or -controlled information systems, to include outsourced business processes supported by private sector information systems and outsourced information technologies; and shall be reviewed and managed relative to contributions to mission outcomes and strategic goals and objectives, in accordance with 40 U.S.C. Sections 1423 and 1451 (reference (l)). Data shall be collected to support reporting and IA management activities across the investment life cycle.

4.4. Interoperability and integration of IA solutions within or supporting the Department of Defense shall be achieved through adherence to an architecture that will enable the evolution to network centric warfare by remaining consistent with the Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance Architecture Framework, and a defense-in-depth approach. This combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response.

4.5. The Department of Defense shall organize, plan, assess, train for, and conduct the defense of DoD computer networks as integrated computer network defense (CND) operations that are coordinated across multiple disciplines in accordance with DoD Directive O-8530.1 (reference (m)).

4.6. Information assurance readiness shall be monitored, reported, and evaluated as a distinguishable element of mission readiness throughout all the DoD Components, and validated by the DoD CIO.

4.7. All DoD information systems shall be assigned a mission assurance category that is directly associated with the importance of the information they contain relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Requirements for availability and integrity are associated with the mission assurance category, while requirements for confidentiality are associated with the information classification or sensitivity and need-to-know. Both sets of requirements are primarily expressed in the form of IA controls and shall be satisfied by employing the tenets of defense-in-depth for layering IA solutions within a given IT asset and among assets; and ensuring appropriate robustness of the solution, as determined by the relative strength of the mechanism and the confidence that it is implemented and will perform as intended. The IA solutions that provide availability, integrity, and confidentiality also provide authentication and non-repudiation.

4.8. Access to all DoD information systems shall be based on a demonstrated need-to-know, and granted in accordance with applicable laws and DoD 5200.2-R (reference (n)) for background investigations, special access and IT position designations and requirements. An appropriate security clearance and non-disclosure agreement are also required for access to classified information in accordance with DoD 5200.1-R (reference (o)). Further:

4.8.1. The minimum requirement for DoD information system access shall be a properly administered and protected individual identifier and password.

4.8.2. The use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication shall be in accordance with published DoD policy and procedures. These technologies shall be incorporated in all new acquisitions and upgrades whenever possible. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the Department of Defense shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.

4.9. In addition to the requirements in paragraph 4.8., foreign exchange personnel and representatives of foreign nations, coalitions or international organizations may be authorized access to DoD information systems containing classified or sensitive information only if all of the following conditions are met:

4.9.1. Access is authorized only by the DoD Component Head in accordance with the Department of Defense, the Department of State (DoS), and DCI disclosure and interconnection policies, as applicable.

4.9.2. Mechanisms are in place to strictly limit access to information that has been cleared for release to the represented foreign nation, coalition or international organization, (e.g., North Atlantic Treaty Organization) in accordance with DoD Directive 5230.11 (reference (p)), for classified information, and other policy guidance for unclassified information such as reference (o), DoD Directive 5230.20*E* (reference (q)), and DoD Instruction 5230.27 (reference (r)).

4.10. Authorized users who are contractors, DoD direct or indirect hire foreign national employees, or foreign representatives as described in paragraph 4.9., above, shall always have their affiliation displayed as part of their e-mail addresses.

4.11. Access to DoD-owned, -operated or -outsourced web sites shall be strictly controlled by the web site owner using technical, operational, and procedural measures appropriate to the web site audience and information classification or sensitivity.

4.11.1. Access to DoD-owned, -operated or -controlled web sites containing official information shall be granted according to reference (o) and need-to-know rules established by the information owner.

4.11.2. Access to DoD-owned, -operated or -controlled web sites containing public information is not restricted; however, the information accessible through the web sites shall be limited to unclassified information that has been reviewed and approved for release in accordance with DoD Directive 5230.9 and DoD Instruction 5230.29 (references (s) and (t)).

4.12. DoD information systems shall regulate remote access and access to the Internet by employing positive technical controls such as proxy services and screened subnets, also called demilitarized zones (DMZ), or through systems that are isolated from all other DoD information systems through physical means. This includes remote access for telework.

4.13. All DoD information systems shall be certified and accredited in accordance with DoD Instruction 5200.40 (reference (u)).

4.14. All interconnections of DoD information systems shall be managed to continuously minimize community risk by ensuring that the assurance of one system is not undermined by vulnerabilities of interconnected systems.

4.14.1. Interconnections of Intelligence Community (IC) systems and DoD information systems shall be accomplished using a process jointly established by the DoD CIO and the IC CIO.

4.14.2. Connection to the Defense Information System Network (DISN) shall comply with connection approval procedures and processes, as established.

4.14.3. Interconnections among DoD information systems of different security domains or with other U.S. Government systems of different security domains shall be employed only to meet compelling operational requirements, not operational convenience. Secure configurations of approved IA and IA-enabled IT products, uniform risk criteria, trained systems security personnel, and strict configuration control shall be employed. The community risk shall be assessed and measures taken to mitigate that risk in accordance with procedures established by the DISN Designated Approving Authorities (DAAs) prior to interconnecting the systems.

4.14.4. The interconnection of DoD information systems with those of U.S. allies, foreign nations, coalition partners, or international organizations shall comply with applicable international agreements and, whenever possible, DoD IA policies. Variations shall be approved by the responsible Combatant Commander and the DISN DAAs, and incorporated in the system security documentation. Information provided through these interconnections must be released in accordance with reference (o) or reference (p).

4.15. All DoD information systems shall comply with DoD ports and protocols guidance and management processes, as established.

4.16. The conduct of all DoD communications security activities, including the acquisition of COMSEC products, shall be in accordance with DoD Directive C-5200.5 (reference (v)).

4.17. All IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DoD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 (reference (w)). Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase; i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period of time specified in the solicitation and the contract. Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National IA Partnership (NIAP) Assurance Maintenance Program.

4.18. All IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines.[1]

4.19. Public domain software products, and other software products with limited or no warranty, such as those commonly known as freeware or shareware, shall only be used in DoD information systems to meet compelling operational requirements. Such products shall be thoroughly assessed for risk and accepted for use by the responsible DAA.

[1] Guidelines are available at http://iase.disa.mil/ and http://www.nsa.gov/

4.20. DoD information systems shall be monitored based on the assigned mission assurance category and assessed risk in order to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or IT resources, including internal misuse. DoD information systems also shall be subject to active penetrations and other forms of testing used to complement monitoring activities in accordance with DoD and Component policy and restrictions.

4.21. Identified DoD information system vulnerabilities shall be evaluated for DoD impact, and tracked and mitigated in accordance with DoD-directed solutions, e.g., Information Assurance Vulnerability Alerts.

4.22. All personnel authorized access to DoD information systems shall be adequately trained in accordance with DoD and Component policies and requirements and certified as required in order to perform the tasks associated with their IA responsibilities.

4.23. Individuals shall be notified of their privacy rights and security responsibilities in accordance with DoD Component General Counsel-approved processes when attempting access to DoD information systems.

4.24. Mobile code technologies shall be categorized and controlled to reduce their threat to DoD information systems in accordance with DoD and Component policy and guidance.

4.25. A DAA shall be appointed for each DoD information system operating within or on behalf of the Department of Defense, to include outsourced business processes supported by private sector information systems and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and have a level of authority commensurate with accepting, in writing, the risk of operating DoD information systems under his or her purview.

4.26. All military voice radio systems, to include cellular and commercial services, shall be protected consistent with the classification or sensitivity of the information transmitted on the system.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense for *Networks and Information Integration*, as the DoD Chief Information Officer, shall:

5.1.1. Monitor, evaluate and provide advice to the Secretary of Defense regarding all DoD IA activities.

5.1.2. Oversee appropriations earmarked for the DoD IA program and manage the supporting activities of the office of the Defense-wide Information Assurance Program (DIAP) Office in accordance with reference (a).

5.1.3. Develop and promulgate additional IA policy guidance consistent with this Directive to address such topics as ports and protocols management, vulnerability management, biometrics, security management, IA education and training, mobile code, and interconnection between security domains.

5.1.4. Ensure the integration of IA initiatives with critical infrastructure protection sector liaisons, as defined in DoD Directive *3020.40* (reference (x)).

5.1.5. Establish a formal coordination process with the IC CIO to ensure proper protection of IC information within the Department of Defense.

5.1.6. Establish metrics and annually validate the IA readiness of all DoD Components as an element of mission readiness.

5.1.7. Ensure that responsibilities for IA aspects of Major Defense Acquisition Program design are integrated into existing Under Secretary of Defense (Acquisition, Technology, and Logistics) (USD(AT&L)) and Service Acquisition Executive processes.

5.1.8. Require the Director, Defense Information Systems Agency (DISA) to:

5.1.8.1. Develop, implement and oversee a single IA approach for layered protection (defense-in-depth) of the DISN in coordination with the Chairman of the Joint Chiefs of Staff, Director, Defense Intelligence Agency (DIA) and Director, National Security Agency (NSA).

5.1.8.2. Establish and manage connection approval processes for the DISN.

5.1.8.3. Develop and provide IA training and awareness products.

5.1.8.4. Develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA.

5.1.8.5. Establish and implement:

5.1.8.5.1. A DoD ports and protocols management process.

5.1.8.5.2. Procedures for mitigation of risks associated with the use of mobile code in DoD information systems.

5.1.8.5.3. A web-based resource providing access to current DoD and Federal IA and IA-related policy and guidance, including recent and pending legislation.

5.1.9. Require the Director, Defense Intelligence Agency to:

5.1.9.1. Provide finished intelligence on IA, including threat assessments, to the DoD Components.

5.1.9.2. Develop, implement, and oversee an IA program for layered protection of the DoD non-cryptologic SCI systems including the DoD Intelligence Information System (DoDIIS) on the basis of defined DoD information systems and geographical or organizational boundaries.

5.1.9.3. Certify and accredit DoD non-cryptologic SCI and DoDIIS applications, enclaves, platform IT interconnections, and outsourced IT-based processes, and develop and provide an IA education, training, and awareness program for DoD non-cryptologic SCI systems and DoDIIS users and administrators.

5.1.9.4. Establish and manage a connection-approval process for the Joint Worldwide Intelligence Communications System.

5.1.10. Require the Director, Defense Security Service to monitor information system security practices and conduct regular inspections of DoD contractors processing classified information in accordance with DoD 5220.22-M (reference (y)).

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) shall:

5.2.1. Require the Director, Defense Research and Engineering (DDR&E) to:

5.2.1.1. Monitor and oversee, in coordination with the Defense-wide Information Assurance Program Office, all Defense-wide IA research and technology investments and activities to include protection mechanisms, detection and monitoring, response and recovery, and IA assessment tools and techniques.

5.2.1.2. Require the Director, Defense Advanced Research Projects Agency (DARPA) to coordinate all DoD IA research and technology initiatives under DARPA's purview with the Director, NSA.

5.2.2. Integrate policies established by this Directive and reference (w) into acquisition policy and guidance to include the Federal Acquisition Regulations System (reference (z)), and incorporate such policies into acquisitions under his or her purview.

5.2.3. Oversee IA assessments, in coordination with the Director, Operational Testing and Evaluation.

5.3. The Under Secretary of Defense for Personnel and Readiness shall, in coordination with the ASD(*NII*), develop and implement IA personnel management and skill tracking procedures and processes to ensure adequate personnel resources are available to meet critical DoD IA requirements.

5.4. The OSD Principal Staff Assistants shall:

5.4.1. Ensure end-to-end protection of information flows in their functional areas by guiding investments and other actions relating to IA.

5.4.2. Ensure that IA requirements for DoD information systems developed under their cognizance are fully coordinated at the DoD Component level and with the DIAP.

5.4.3. Appoint DAAs for Joint and Defense-wide information systems under their purview (e.g., the Defense Civilian Personnel Data System, Defense Message System, Defense Travel System, and the Joint Total Asset Visibility System).

5.4.4. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems under their purview.

5.5. The Secretary of the Army shall serve as the Executive Agent for the integration of common biometric technologies throughout the Department of Defense.

5.6. The Chairman of the Joint Chiefs of Staff shall:

5.6.1. Serve as the principal military advisor to the Secretary of Defense on IA.

5.6.2. Ensure, in coordination with the ASD(*NII*), the validation of IA requirements for systems supporting Joint and Combined operations through the Joint Requirements Oversight Council.

5.6.3. Develop, coordinate, and promulgate IA policies, doctrine and procedures for Joint and Combined operations.

5.7. The Commander, United States Strategic Command, shall coordinate and direct DoD-wide CND operations in accordance with reference (m).

5.8. The Director, National Security Agency (NSA), shall:

5.8.1. Implement an IA intelligence capability responsive to requirements for the Department of Defense, less DIA responsibilities.

5.8.2. Provide IA support to the DoD Components as required in order to assess the threats to, and vulnerabilities of, information technologies.

5.8.3. Serve as the DoD focal point for IA cryptographic research and development in accordance with DDR&E direction and in coordination with the Director, DARPA.

5.8.4. Manage the development of the IA Technical Framework (reference (a*a)*) in support of defense-in-depth, and provide engineering support and other technical assistance for its implementation within the Department of Defense.

5.8.5. Serve as the DoD focal point for the NIAP and establish criteria and processes for evaluating and validating all IA and IA-enabled IT products used in DoD information systems.

5.8.6. Plan, design, and manage the implementation of the Key Management Infrastructure/PKI within the Department of Defense.

5.8.7. In coordination with the USD(AT&L), develop and maintain an information system security engineering process that supports IT acquisition.

5.8.8. Support the Director, Defense Information Systems Agency in the development of security configuration guidance for IA and IA-enabled IT products.

5.8.9. Develop, implement, and oversee an IA program for layered protection of DoD cryptologic SCI systems, an IA certification and accreditation process for DoD cryptologic SCI applications, enclaves, platform IT interconnections and outsourced IT-based processes, and an IA education, training, and awareness program for users and administrators of DoD cryptologic SCI systems.

5.9. The Director, Operational Testing and Evaluation, shall oversee IA assessments.

5.10. The Heads of the DoD Components shall:

5.10.1. Develop and implement an IA program focused on assurance of DoD Component-specific information and systems (e.g., sustaining base, tactical, and Command, Control, Communications, Computers, and Intelligence (C4I) interfaces to weapon systems) that is consistent with references (a) and (l) and defense-in-depth.

5.10.2. Coordinate with Joint and Defense-wide program offices to ensure interoperability of IA solutions across the DoD enterprise.

5.10.3. Collect and report IA management, financial, and readiness data to meet DoD IA internal and external reporting requirements.

5.10.4. Appoint DAAs for all DoD information systems for which they have responsibility.

5.10.5. Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or replacement of all DoD information systems for which they have responsibility.

5.10.6. Ensure that the Government's contract requirements properly reflect that IA or IA-enabled IT products are involved and must be properly evaluated and validated in accordance with paragraph 4.17., above.

5.10.7. Ensure that IA awareness, training, education, and professionalization are provided to all Component personnel commensurate with their respective responsibilities for developing, using, operating, administering, maintaining, and retiring DoD information systems.

5.10.8. Comply with established accreditation and connection approval processes required for all DoD information systems.

5.10.9. Coordinate all IA research and technology initiatives under their purview with the DDR&E.

6. EFFECTIVE DATE

This Directive is effective immediately.

Paul Wolfowitz

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures - 2
E1. References, continued
E2. Definitions

E1. ENCLOSURE 1

REFERENCES, continued

(e) DoD CIO Memorandum 6-8510, "Guidance and Policy for Department of Defense Global Information Grid Information Assurance," June 16, 2000 (hereby canceled)
(f) DoD 5025.1-M, "DoD Directives System Procedures," *March 5, 2003*
(g) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
(h) DoD Directive *5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005*
(i) National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000[2]
(j) OMB Circular A-130, "Management of Federal Information Resources, Transmittal 4," November 30, 2000
(k) DoD Directive 5000.1, "The Defense Acquisition System," *May 12, 2003*
(l) Sections 1423 and 1451 of title 40, United States Code, "Division E of the Clinger-Cohen Act of 1996"
(m) DoD Directive O-8530.1, "Computer Network Defense," January 8, 2001
(n) DoD 5200.2-R, "DoD Personnel Security Program," *December 16, 1986*
(o) DoD 5200.1-R, "DoD Information Security Program Regulation," January 14, 1997
(p) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(q) DoD Directive 5230.20*E*, "Visits *and* Assignments of Foreign Nationals," *June 22, 2005*
(r) DoD Instruction 5230.27, "Presentation of DoD-Related Scientific and Technical Papers at Meetings," October 6, 1987
(s) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," April 9, 1996
(t) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 6, 1999
(u) DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process (DITSCAP)," December 30, 1997
(v) DoD Directive C-5200.5, "Communications Security (COMSEC)," (U) April 21, 1990
(w) National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, "National Policy Governing the Acquisition of Information Assurance (IA) and IA-enabled Information Technology Products," January 2000
(x) DoD Directive *3020.40, "Defense Critical Infrastructure Program (DCIP)," August 19, 2005*
(y) DoD 5220.22-M, "National Industrial Security Program Operating Manual," January 1995 and "National Industrial Security Program Operating Manual Supplement," February 1995

[2] Available at http://www.nstissc.gov/html/library.html

(z) Title 48, Code of Federal Regulations, "Federal Acquisition Regulations System," October 1, 19963[3]

(a*a*) Information Assurance Technical Framework (IATF), Release 3.0, September 2000[4]

(a*b*) DoD 7000.14-R, Vol 2B, Chapter 5, "DoD Financial Management Regulation," June 2000

(a*c*) Section 552a of title 5, United States Code, "The Privacy Act of 1974"

(a*d*) Section 278g-3 of title 15, United States Code, "Computer Security Act of 1987"

(a*e*) DoD 5400.7-R, "DoD Freedom of Information Act Program," September 4, 1998

(a*f*) Section 552 of title 5, United States Code, "Freedom of Information Act"

(a*g*) DoD Directive 5210.83, "Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI)", November 15, 1991

(a*h*) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

[3] Available at http://web1.deskbook.osd.mil/htmlfiles/rlcats.asp

[4] Available at http://www.iatf.net

E2. ENCLOSURE 2

DEFINITIONS

E2.1.1. Application. Software program that performs a specific function directly for a user and can be executed without access to system control, monitoring or administrative privileges. Examples include office automation, electronic mail, web services, and major functional or mission software programs.

E2.1.2. Authentication. Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information (reference (i)).

E2.1.3. Authorized User. Any appropriately cleared individual with a requirement to access a DoD information system in order to perform or assist in a lawful and authorized governmental function.

E2.1.4. Availability. Timely, reliable access to data and information services for authorized users (reference (i)).

E2.1.5. Community Risk. Probability that a particular vulnerability will be exploited within an interacting population and adversely impact some members of that population.

E2.1.6. Computer Network. The constituent element of an enclave responsible for connecting computing environments by providing short-haul data transport capabilities such as local or campus area networks, or long-haul data transport capabilities such as operational, metropolitan, or wide area and backbone networks.

E2.1.7. Computing Environment. Workstation or server (host) and its operating system, peripherals, and applications (reference (i)).

E2.1.8. Confidentiality. Assurance that information is not disclosed to unauthorized entities or processes (reference (i)).

E2.1.9. Connection Approval. Formal authorization to interconnect information systems.

E2.1.10. Controlled Unclassified Information. A term used, but not specifically defined in reference (o), to refer to sensitive information as defined in paragraph E2.1.41., below.

E2.1.11. Defense-in-Depth. The DoD approach for establishing an adequate IA posture in a shared-risk environment that allows for shared mitigation through: the integration of people, technology, and operations; the layering of IA solutions within and among IT assets; and, the selection of IA solutions based on their relative level of robustness.

E2.1.12. Defense Information System Network (DISN). The DoD consolidated worldwide enterprise-level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations.

E2.1.13. Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority (reference (i)).

E2.1.14. DISN Designated Approving Authority (DISN DAA). One of four DAAs responsible for operating the DISN at an acceptable level of risk. The four DISN DAAs are the Directors of the DISA, the DIA, the NSA and the Director of the Joint Staff (delegated to the Joint Staff Director for Command, Control, Communications, and Computer Systems (J-6)).

E2.1.15. DMZ (Demilitarized Zone). Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's IA policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks. A DMZ is also called a "screened subnet."

E2.1.16. DoD Information System. Set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

E2.1.16.1. Automated Information System (AIS) Application. For DoD information assurance purposes, an AIS application is the product or deliverable of an acquisition program, such as those described in reference (k). An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support); multiple software applications that are related to a single mission (e.g., payroll or personnel); or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense

Messaging System). AIS applications are deployed to enclaves for operations, and have their operational security needs assumed by the enclave. Note that an AIS application is analogous to a "major application" as defined in reference (j); however, this term is not used in order to avoid confusion with the DoD acquisition category of Major Automated Information System.

E2.1.16.2. Enclave. Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems as defined in reference (j). Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

E2.1.16.3. Outsourced IT-based Process. For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

E2.1.16.4. Platform IT Interconnection. For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition, and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

E2.1.17. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

E2.1.18. IA Certification and Accreditation. The standard DoD approach for identifying information security requirements, providing security solutions, and managing the security of DoD information systems.

E2.1.19. IA Control. An objective IA condition of integrity, availability or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format, i.e., a control number, a control name, control text, and a control class. Specific management, personnel, operational, and technical controls are applied to each DoD information system to achieve an appropriate level of integrity, availability, and confidentiality in accordance with reference (j).

E2.1.20. IA Product. Product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control, non-repudiation of data); correct known vulnerabilities; and/or provide layered defense against various categories of non-authorized or malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls, and intrusion detection devices.

E2.1.21. IA-Enabled Information Technology Product. Product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. Examples include such products as security-enabled web browsers, screening routers, trusted operating systems, and security-enabled messaging systems.

E2.1.22. Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

E2.1.23. Integrity. Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (reference (i)).

E2.1.24. IT Position Category. Applicable to unclassified DoD information systems, a designator that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. Position categories include: IT-I (Privileged), IT-II (Limited Privileged) and IT-III (Non-Privileged), as defined in reference (o). Investigative requirements for each category vary, depending on role and whether the incumbent is a U.S. military member, U.S. civilian government employee, U.S. civilian contractor or a foreign national. The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position.

E2.1.25. Mission Assurance Category (MAC). Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories:

E2.1.25.1. Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

E2.1.25.2. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.

E2.1.25.3. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.

E2.1.26. Mobile Code. Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

E2.1.27. National Information Assurance Partnership (NIAP). Joint initiative between the NSA and the National Institute of Standards and Technology responsible for security testing needs of both IT consumers and producers and promoting the development of technically sound security requirements for IT products and systems and appropriate measures for evaluating those products and systems.

E2.1.28. Need-to-Know. Necessity for access to, or knowledge or possession of, specific official DoD information required to carry out official duties (reference (i) modified).

E2.1.29. Need-to-Know Determination. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties (reference (i)).

E2.1.30. Non-repudiation. Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data (reference (i)).

E2.1.31. Official DoD Information. All information that is in the custody and control of the Department of Defense, relates to information in the custody and control of the Department, or was acquired by DoD employees as part of their official duties or because of their official status within the Department (reference (s)).

E2.1.32. Portfolio. The aggregate of IT investments for DoD information systems, infrastructure and related technical activities that are linked to mission goals, strategies, and architectures, using various assessment and analysis tools to permit information and IT decisions to be based on their contribution to the effectiveness and efficiency of military missions and supporting business functions. Portfolios enable the Department of Defense to manage IT resources and align strategies and programs with Defense-wide, functional, and organizational goals and measures.

E2.1.33. Proxy. Software agent that performs a function or operation on behalf of another application or system while hiding the details involved. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client network address is authorized to use the requested service, optionally perform additional authentication, and then complete a connection on behalf of the user to a remote destination.

E2.1.34. Public Domain Software. Software not protected by copyright laws of any nation that carries no warranties or liabilities, and may be freely used without permission of or payment to the creator.

E2.1.35. Public Information. Official DoD information that has been reviewed and approved for public release by the information owner in accordance with reference (s).

E2.1.36. Research and Technology. Activities that may be described as basic research, applied research, and advanced technology development, demonstrations or equivalent activities, regardless of budget activity. Definitions for Basic Research, Applied Research and Advanced Technology Development are provided in the DoD FMR, Chapter 5 (reference (a*b*)).

E2.1.37. Robustness. A characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly. The Department of Defense has three levels of robustness:

E2.1.37.1. High Robustness: Security services and mechanisms that provide the most stringent protection and rigorous security countermeasures.

E2.1.37.2. Medium Robustness: Security services and mechanisms that provide for layering of additional safeguards above good commercial practices.

E2.1.37.3. Basic Robustness: Security services and mechanisms that equate to good commercial practices.

E2.1.38. Security Domain. Within an information system, the set of objects that is accessible. Access is determined by the controls associated with information properties such as its security classification, security compartment or sensitivity. The controls are applied both within the information system and in its connection to other classified or unclassified information systems.

E2.1.39. Sensitive But Unclassified (SBU). A term commonly and inappropriately used within the Department of Defense as a synonym for Sensitive Information, which is the preferred term.

E2.1.40. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of Central Intelligence.

E2.1.41. Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act" (reference (a*c*)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987" (reference (a*d*)).) This includes information in routine DoD payroll, finance, logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to the following:

E2.1.41.1. For Official Use Only (FOUO). In accordance with DoD 5400.7-R (reference (a*e*)), DoD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) (reference (a*f*)).

E2.1.41.2. Privacy Data. Any record that is contained in a system of records, as defined in the reference (a*c*) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

E2.1.41.3. DoD Unclassified Controlled Nuclear Information (DoD UCNI). Unclassified information on security measures (security plans, procedures and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83 (reference (a*g*)). Information is Designated DoD UCNI when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

E2.1.41.4. Unclassified Technical Data. Data that is not classified, but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25 (reference (a*h*)).

E2.1.41.5. Proprietary. Information that is provided by a source or sources under the condition that it not be released to other sources.

E2.1.41.6. Foreign Government Information. Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with reference (o).

E2.1.41.7. Department of State Sensitive But Unclassified (DoS SBU). Information which originated from the DoS that has been determined to be SBU under appropriate DoS information security polices.

E2.1.41.8. Drug Enforcement Administration (DEA) Sensitive Information. Information originated by the DEA that requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

E2.1.42. Supporting IA Infrastructures. Collections of interrelated processes, systems, and networks that provide a continual flow of information assurance services throughout the Department of Defense, e.g., the key management infrastructure or the incident detection and response infrastructure.

E2.1.43. Telework. Any arrangement in which an employee performs officially assigned duties at an alternative worksite on either a regular and recurring, or on an ad hoc, basis (not including while on official travel).

ARTICLE 29 DATA PROTECTION WORKING PARTY

1271-04-02/08/EN
WP 155 rev.04

Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules

Adopted on 24 June 2008
As last Revised and adopted on 8 April 2009

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/06.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

FAQs on Binding Corporate Rules (BCR)

As explained in Working Paper 74 (WP 74)[1], the Article 29 working party considers that BCRs are an appropriate solution for multinational companies and other such groups to meet their legal obligations and ensure a proper level of protection of personal information when transferring data out of the European Union.

The working party/Data Protection Authorities have published these FAQs in light of their experience of the applications made for approval of BCRs and enquiries received about the interpretation of documents WP 74[2] and WP 108[3]. The FAQs are intended to clarify particular requirements for applicants in order to assist them in gaining approval for their BCRs.

These FAQs are not exhaustive and will be updated as required.

1 – Do the BCRs have to apply to all the personal data processed by the group?

No, BCRs are a legal means for providing adequate protection to personal data which is covered by Directive 95/46/EC and transferred out of the European Union to countries that are not considered to provide an adequate level of protection. Other personal data processed by the group, which is not processed at some point in the EU, does not have to be covered by the rules.

However, it is strongly recommended that multinational groups using BCRs have a single set of global policies or rules in place to protect all the personal data that they process. Having a single set of rules will create a simpler and more effective system which will be easier for staff to implement and for data subjects to understand. Companies are likely to be respected for demonstrating a firm commitment to a high level of privacy for all data subjects regardless of their location and the legal requirements in any particular jurisdiction.

It should be noted that it is possible for the group to have a single set of rules while at the same time limiting the third party beneficiary rights required in the BCRs only to personal data transferred from the European Union.

2 –Do the BCRs have to apply to data processors who are not part of the group?

No, only processors who are part of the group and are processing data on behalf of other members of the group will have to respect the BCRs as a member of the group. The BCRs could contain particular rules dedicated to members of the group acting as processors as a means of meeting the requirements of Articles 16 and 17 of Directive 95/46/EC.

[1] Working Document WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on June 3, 2003 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm

[2] See footnote 1

[3] Working Document WP 108: Establishing a model checklist application for approval of Binding Corpate Rules, adopted on April 14, 2005 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

Processors who are not part of the group and act on behalf of a group member are not required to be bound by the BCR. However, those processors should always only act under the instructions of the controller and should be bound by contract or other legal act in line with the provisions of the Articles 16 and 17 of the EU Directive.

If the processors are not part of the group and are based outside of the EU, the members of the group will also have to comply with the Articles 25 and 26 of Directive 95/46/EC on transborder data flows and ensure an adequate level of protection. For instance, the company can seek to adduce adequacy by contractual means such as by making use of the Standard Contractual Clauses adopted by the EU Commission for transfers to a processor outside of the EU or by subjecting the processors to the BCRs' provisions in respect of their data.

The BCRs will need to address these situations.

3 – Where a breach of the BCR occurs outside the EU which member of the group is liable?

Regardless of the existence of any liability under Directive 95/46/EC for the entity that exports personal data from the EU, the BCRs themselves must nominate an entity within the EU who accepts liability for any breaches of the rules by any member of the group outside of the EU. This liability only needs to extend to data transferred from the EU under the rules.

WP74 envisaged that in most cases it would be the headquarters of the group, if EU based, that would accept liability. Where the headquarters of the group is based outside of the EU, WP74 allowed the group to nominate a suitable member in the EU who would accept liability for breaches of the rules outside of the EU. This responsibility includes, but is not limited to, the payment for any damages resulting from the violation of the binding corporate rules by any member outside of the EU bound by the rules.

However, for some groups with particular corporate structures, it is not always possible to impose to a specific entity to take all the responsibility for any breach of BCRs out of the EU. In these cases, the working party accepts that where the group can demonstrate why it is not possible for them to nominate a single entity in the EU they can propose other mechanisms of liability that better fit the organization.

One possibility would be to create a joint liability mechanism between the data importers and the data exporters as seen in the EU Standard Contractual Clauses 2001/497/EC dated June 15, 2001 or to define an alternative liability scheme based on due diligence obligations as prescribed in the EU Standard Contractual Clauses 2004/915/EC dated December 27, 2004. A last possibility, specifically dedicated to transfers made from controllers to processors is the application of the liability mechanism of the Standard Contractual Clauses 2002/16/EC dated December 27, 2001.

Data protection authorities may accept those alternative solutions mentioned above to liability on a case-by-case basis where sufficient and adequate comfort is provided by the applicant. Where any alternative mechanism is used it is important to show that the data subjects will be assisted in exercising their rights and not disadvantaged or unduly inhibited in any way.

4 – Should the BCR always contain a right for the data subject to lodge a complaint before the data protection authority for violation of the BCR?

Yes, despite the fact that in some cases the rules or the third party beneficiary rights in particular may have been limited to data originating from the EU and individuals already have a right in their national law to make a complaint about the exporting entity to the data protection authority it is important to have a right to lodge a complaint on the face of the BCRs for a breach of the rules as a whole by any member of the group.

5 – Should information about third party beneficiary rights be made readily available to the data subjects that benefit from it?

Yes, WP74 requires that both the BCRs and the ways to complain and seek a remedy for a breach of the rules should be easily accessible for the data subject. The existence of third party beneficiary rights and their content is an important option for a data subject when considering what remedies are available to them. Some companies have decided for legitimate reasons not to include the third party beneficiary rights clause in the core document of the BCRs but instead set the rights out in a separate document. In those cases where the rights are in a separate document they should be made transparent and easily accessible to any data subject benefiting from those rights.

6 - Do the BCR themselves have to describe the processing and transfers of personal data within the group and in what level of detail?

Yes, a general description of the main purposes of processing and types of data transfers will need to be included in the BCR.

For example, the group can explain in its BCR that transfers are made to all entities of the group for staff mobility reasons, that HR data are sent to the main data centres of the group in Germany, US and Singapore for storage and archiving, that HR data are sent to the headquarters to define global compensation strategy and benefits planning for the group.

However, when applying for national authorisation and permit requirements, some Member States may require applicants to list the individual transfers that will take place from their jurisdiction to third countries into national filing documents.

7 - Should the BCRs be set out in a single document that creates all obligations of the group and the rights of individuals?

It would greatly facilitate the review of BCRs by Data Protection Authorities and at the same time make BCRs more transparent for data subjects if there was one document showing clearly all obligations and rights which, if necessary, should be complemented by additional and relevant documentation (e.g. policies, guidelines, audit/training programmes). This structure is proposed as an example in the WP.154 adopted in June 24, 2008 providing a framework for BCRs. Although it is not obligatory to have BCRs in a single document.

8 – What terminology should applicants use for drafting their BCR?

As BCR are a tool, with internal and external legal effects, that provide a level of data protection which is adequate under the EU Directive 95/46/EC, the wording and definitions of the BCR key principles (as listed in WP.74, WP.108, WP.153 and WP.154) should be consistent with the wording and definitions of the EU Directive.
This avoids misinterpretation of the BCR and assists when seeking authorisation from a Data Protection Authority as they are easily understood.
This does not prevent companies from using different language – with the same meaning, however – if this is easier for the staff and for client to understand when implementing the BCR into group policies or internal guidelines.

9 – What rights should an individual have under the third party beneficiary rights clause?

An individual whose personal data are processed under the BCR can enforce the following BCR principles as rights before the appropriate data protection authority or court according to the rules defined by the WP. 74, WP. 108, and WP153, in order to seek remedy and obtain compensation if a member of the group has not met the obligations and does not respect those principles.

More specifically, the principles which are enforceable as third party beneficiary rights are as follows:

- Purpose limitation (WP 153 Section 6.1, WP 154 Section 3),
- Data quality and proportionality (WP 153 Section 6.1, WP 154 Section 4),
- Criteria for making the processing legitimate (WP 154 Sections 5 and 6),
- Transparency and easy access to BCR (WP 153 Section 6.1, Section 1.7, WP 154 Section 7),
- Rights of access, rectification, erasure, blocking of data and object to the processing (WP 153 Section 6.1, WP 154 Section 8),
- Rights in case automated individual decisions are taken (WP 154 Section 9)
- Security and confidentiality (WP 153 Section 6.1,WP 154 Sections 10 and 11),
- Restrictions on onward transfers outside of the group of companies (WP 153 Section 6.1, WP 154 Section 12),
- National legislation preventing respect of BCR (WP 153 Section 6.3, WP 154 Section 16),
- Right to complain through the internal complaint mechanism of the companies (WP 153 Section 2.2, WP 154 Section 17),
- Cooperation duties with Data Protection Authority (WP. 153 Section 3.1, WP 154 Section 20),
- Liability and jurisdiction provisions (WP. 153 Section 1.3, 1.4 , WP 154 Sections 18 and 19),

Companies should ensure that all those rights are covered by the third party beneficiary clause of their BCR by, for example, making a reference to the clauses/sections/parts of their BCR where these rights are regulated in or by listing them all in the said third party beneficiary clause.

These rights do not extend to those elements of the BCR pertaining to internal mechanisms implemented within entities such as detail of training, audit programmes, compliance network, and mechanism for updating of the rules. [WP153 Section 2.1, 2.3, 2.4 and 5.1, WP.154 Sections 13 to 15 included and Section 21]

10 – What is the relationship between EEA data protection laws and BCRs?

BCRs do not substitute EEA national data protection laws, applying to the processing of personal data in EEA Member States. Although BCRs shall provide adequate safeguards for the transfers of personal data, they should not be considered as an instrument to replace EEA data protection laws. Indeed, an authorization given by an EEA Member State under Article 26 (2) of Directive 95/46/EC exclusively addresses international transfers from an EEA Member State to third countries and does therefore not certify that the processing activities taking place in the EEA are compliant with EEA national data protection laws.

11 – What does the reversal of the burden of proof mean in practice?

Where data subjects can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of BCR, it will be for the member of the group in Europe that accepted liability to prove that the member of the corporate group outside of Europe was not responsible for the breach of the BCR giving rise to those damages or that no such breach took place.

Done at Brussels, on 24/06/2008

For the Working Party
The Chairman
Alex TÜRK

As last revised and adopted on 08/04/2009

For the Working Party
The Chairman
Alex TÜRK

NIST Special Publication 800-53
Revision 3

Recommended Security Controls for Federal Information Systems and Organizations

National Institute of Standards and Technology
U.S. Department of Commerce

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2009
INCLUDES UPDATES AS OF 08-12-2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Special Publication 800-53, Revision 3, 237 pages

(August 2009)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

Compliance with NIST Standards and Guidelines

In accordance with the provisions of FISMA,[1] the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems. The Secretary shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems. Standards prescribed shall include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

- Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies.[2] FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.
- Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management), state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.[3]
- Other security-related publications, including interagency reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when specified by OMB.
- Compliance schedules for NIST security standards and guidelines are established by OMB.

[1] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

[3] While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies should apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. When assessing federal agency compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors, should consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government—including a consistent process for selecting and specifying safeguards and countermeasures (i.e., security controls) for federal information systems. The Project Leader, Ron Ross, from the National Institute of Standards and Technology, wishes to acknowledge and thank the senior leadership team from the U.S. Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to the publication. The senior leadership team, working group members, and their organizational affiliations include:

U.S. Department of Defense

Cheryl J. Roby
Assistant Secretary of Defense
DOD Chief Information Officer (Acting)

Robert Lentz
Deputy Assistant Secretary of Defense
for Cyber, Identity, and Information Assurance

Gus Guissanie
Principal Director, ODASD (CIIA)

Don Jones
Senior Policy Advisor, ODASD (CIIA)

Office of the Director of National Intelligence

Honorable Priscilla Guthrie
Associate Director of National Intelligence
and Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief
Information Officer

Mark J. Morrison
Deputy Associate Director of National
Intelligence for IC Information Assurance

Roger Caslow
Lead, C&A Transformation

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Cheryl J. Roby
Chairman, Committee on National Security
Systems (Acting)

Eustace D. King
CNSS Subcommittee Co-Chairman (DOD)

William Hunteman
CNSS Subcommittee Co-Chairman (DOE)

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross
NIST, JTF Leader

Marianne Swanson
NIST

Stuart Katzke
NIST

Gary Stoneburner
Johns Hopkins APL

Richard Graubart
MITRE Corporation

Glenda Turner
MITRE Corporation

Esten Porter
MITRE Corporation

Bennett Hodge
Booz Allen Hamilton

Kelley Dempsey
NIST

George Rogers
BAE Systems, Inc.

Arnold Johnson
NIST

Christian Enloe
NIST

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support; to Donna Dodson, Pat Toth, Matt Scholl, Sharon Keller, Randy Easter, Tim Polk, Murugiah Souppaya, Kevin Stine, Matt Barrett, Steve Quinn, Bill MacGregor, Karen Scarfone, Bill Burr, Doug Montgomery, Scott Rose, Mark Wilson, Annabelle Lee, Ed Roback, and Erika McCallister for their review of the security controls and insightful recommendations. The authors also wish to recognize Marshall Abrams, Jennifer Fabius Greene, Harriett Goldman, John Woodward, Karen Quigg, Joe Weiss, Peter Gouldmann, Roger Johnson, Sarbari Gupta, Dennis Bailey, Richard Wilsher, Nadya Bartol, Mike Rubin, Tom Madden, Denise Farrar, Paul Bicknell, Robert Niemeyer, and Brett Burley for their exceptional contributions in helping to improve the content of the publication. And finally, the authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, both nationally and internationally, whose thoughtful and constructive comments improved the overall quality and usefulness of this publication.

A special acknowledgment is given to the participants in the *Industrial Control System (ICS) Security Project* who have put forth significant effort in helping to augment the security controls in NIST Special Publication 800-53 for industrial control systems. These participants include: Keith Stouffer, Stu Katzke, and Marshall Abrams from the ICS Security Project Development Team; federal agencies participating in the ICS workshops; and individuals and organizations in the public and private sector ICS community providing insightful comments on the proposed augmentations.

Postscript

Making any significant changes to the publication without public review is not in keeping with the obligation we have to the public and private sector organizations employing the NIST standards and guidelines. Some thoughtful and insightful recommendations received during the final public comment period suggesting changes to the publication have been retained and deferred until the next major revision to Special Publication 800-53. We continue to balance the need for stability in the NIST publications to ensure cost-effective implementation with the need to keep the publications current.

FIPS 200 AND SP 800-53

IMPLEMENTING INFORMATION SECURITY STANDARDS AND GUIDELINES

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a mandatory federal standard developed by NIST in response to FISMA. To comply with the federal standard, organizations must first determine the security category of their information system in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, derive the information system impact level from the security category in accordance with FIPS 200, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security Controls for Federal Information Systems and Organizations*. Organizations have flexibility in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53. This allows organizations to tailor the relevant security control baseline so that it more closely aligns with their mission and business requirements and environments of operation.

FIPS 200 and NIST Special Publication 800-53, in combination, help ensure that appropriate security requirements and security controls are applied to all federal information and information systems. An organizational assessment of risk validates the initial security control selection and determines if any additional controls are needed to protect organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. The resulting set of security controls establishes a level of security due diligence for the organization.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by FISMA, NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST publications are complementary with the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is collaborating with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. A common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their support contractors, more uniform and consistent ways to manage the risk to organizational operations and assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. A common foundation for information security will also provide a strong basis for reciprocal acceptance of security authorization decisions and facilitate information sharing. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Table of Contents

Prologue

"…Through the process of risk management, leaders must consider risk to US interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations… "

"…For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations…"

"…Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain…"

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

Errata

The following changes have been incorporated into Special Publication 800-53, Revision 3, as of date indicated in table.

DATE	TYPE	CHANGE	PAGE NO.
08-12-2009	Editorial	Concatenate AC-19 d. and AC-19 e.	Page F-17
08-12-2009	Editorial	Change AC-19 f. to AC-19 e.	Page F-17
08-12-2009	Editorial	Change AC-19 g. to AC-19 f.	Page F-17
08-12-2009	Editorial	Change AC-19 h. to AC-19 g.	Page F-17

CHAPTER ONE

INTRODUCTION

THE NEED FOR SECURITY CONTROLS TO PROTECT INFORMATION AND INFORMATION SYSTEMS

The selection and implementation of appropriate *security controls* for an information system[4] or a system-of-systems[5] are important tasks that can have major implications on the operations[6] and assets of an organization[7] as well as the welfare of individuals and the Nation. Security controls are the management, operational, and technical safeguards or countermeasures employed within an organizational information system to protect the confidentiality, integrity, and availability of the system and its information. There are several important questions that should be answered by organizational officials when addressing the security considerations for their information systems:

- What security controls are needed to adequately mitigate the risk incurred by the use of information and information systems in the execution of organizational missions and business functions?
- Have the selected security controls been implemented or is there a realistic plan for their implementation?
- What is the desired or required level of assurance (i.e., grounds for confidence) that the selected security controls, as implemented, are effective[8] in their application?

The answers to these questions are not given in isolation but rather in the context of an effective *information security program* for the organization that identifies, mitigates as deemed necessary, and monitors on an ongoing basis, risks[9] arising from its information and information systems. The security controls defined in this publication and recommended for use by organizations in protecting their information systems should be employed in conjunction with and as part of a well-defined and documented information security program. The program management controls (Appendix G), complement the security controls for an information system (Appendix F) by focusing on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs.

[4] An information system is a discrete set of *information resources* organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching/private branch exchange (PBX) systems, and environmental control systems.

[5] In certain situations within an organization, an information system can be viewed from both a logical and physical perspective as a complex *system-of-systems* (e.g., Federal Aviation Administration National Air Space System) when there are multiple information systems involved with a high degree of connectivity and interaction among the systems.

[6] Organizational operations include mission, functions, image, and reputation.

[7] The term *organization* describes an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

[8] Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.

[9] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation.

It is of paramount importance that responsible officials understand the risks and other factors that could adversely affect organizational operations and assets, individuals, other organizations, and the Nation.[10] These officials must also understand the current status of their security programs and the security controls planned or in place to protect their information and information systems in order to make informed judgments and investments that mitigate risks to an acceptable level. The ultimate objective is to conduct the day-to-day operations of the organization and to accomplish the organization's stated missions and business functions with what the OMB Circular A-130 defines as *adequate security*, or security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

1.1 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*. The guidelines apply to all components[11] of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems and effective risk management within the federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations;
- Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*;
- Providing a stable, yet flexible catalog of security controls for information systems and organizations to meet current organizational protection needs and the demands of future protection needs based on changing requirements and technologies;
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness; and
- Improving communication among organizations by providing a common lexicon that supports discussion of risk management concepts.

The guidelines in this special publication are applicable to all federal information systems[12] other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials exercising policy authority over such systems.[13] State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.

[10] Includes risk to U.S. critical infrastructure/key resources as described in Homeland Security Presidential Directive 7.

[11] Information system components include, for example, mainframes, workstations, servers (e.g., database, electronic mail, authentication, web, proxy, file, domain name), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications.

[12] A federal information system is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[13] CNSS Instruction 1253 provides implementing guidance for NIST Special Publication 800-53 for *national security systems*.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse audience of information system and information security professionals including:

- Individuals with information system or security management and oversight responsibilities (e.g., authorizing officials, chief information officers, senior information security officers,[14] information system managers, information security managers);
- Individuals with information system development responsibilities (e.g., program and project managers, information technology product developers, information system designers and developers, systems integrators);
- Individuals with information security implementation and operational responsibilities (e.g., mission/business owners, information system owners, common control providers, information owners/stewards, information system security engineers, information system administrators, information system security officers); and
- Individuals with information system and information security assessment and monitoring responsibilities (e.g., auditors, Inspectors General, system evaluators, assessors/assessment teams, independent verification and validation assessors, information system owners).

Commercial companies producing information technology products and systems, creating information security-related technologies, and providing information security services can also benefit from the information in this publication.

1.3 RELATIONSHIP TO OTHER SECURITY CONTROL PUBLICATIONS

To create a technically sound and broadly applicable set of security controls for information systems and organizations, a variety of sources were considered during the development of this special publication. The sources included security controls from the defense, audit, financial, healthcare, and intelligence communities as well as controls defined by national and international standards organizations. The objective of NIST Special Publication 800-53 is to provide a set of security controls that can satisfy the breadth and depth of security requirements[15] levied on information systems and organizations and that is consistent with and complementary to other established information security standards.

The catalog of security controls provided in Special Publication 800-53 can be effectively used to demonstrate compliance with a variety of governmental, organizational, or institutional security requirements. It is the responsibility of organizations to select the appropriate security controls, to implement the controls correctly, and to demonstrate the effectiveness of the controls in satisfying their stated security requirements. The security controls in the catalog facilitate the development of assessment methods and procedures that can be used to demonstrate control effectiveness in a consistent and repeatable manner—thus contributing to the organization's confidence that there is ongoing compliance with its stated security requirements.[16]

[14] At the *agency* level, this position is known as the Senior Agency Information Security Officer. Organizations may also refer to this position as the *Senior Information Security Officer* or the *Chief Information Security Officer*.

[15] Security requirements are those requirements levied on an information system that are derived from laws, Executive Orders, directives, policies, instructions, regulations, standards, guidelines, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

[16] NIST Special Publication 800-53A provides guidance on assessing the effectiveness of security controls defined in this publication.

1.4 ORGANIZATIONAL RESPONSIBILITIES

Organizations[17] use FIPS 199 to categorize their information and information systems. Security categorization is accomplished as an organization-wide activity[18] with the involvement of senior-level organizational officials including, for example, authorizing officials, chief information officers, senior information security officers, information owners/stewards, information system owners, and risk executive (function). As required by FIPS 200, organizations use the security categorization results to designate information systems as low-impact, moderate-impact, or high-impact systems. For each information system, the recommendation for minimum security controls from Special Publication 800-53 (i.e., the *baseline* security controls defined in Appendix D, adjusted in accordance with the *tailoring* guidance in Section 3.3) is intended to be used as a starting point for and as input to the organization's security control *supplementation* process.[19]

While the FIPS 199 security categorization associates the operation of the information system with the potential adverse impact on organizational operations and assets, individuals, other organizations, and the Nation,[20] the incorporation of refined threat and vulnerability information during the risk assessment facilitates the selection of additional security controls *supplementing* the tailored baseline to address specific organizational needs and tolerance for risk. The final, agreed-upon[21] set of security controls is documented with appropriate rationale in the security plan for the information system. The use of security controls from Special Publication 800-53 and the incorporation of tailored baseline controls as a starting point in the control selection process, facilitate a more consistent level of security across federal information systems and organizations. It also offers the needed flexibility to appropriately modify the controls based on specific organizational policies and requirements, particular conditions and circumstances, known threat and vulnerability information, and tolerance for risk.

Building more secure information systems is a multifaceted undertaking that requires:

- Well-defined security requirements and security specifications;
- Well-designed and well-built information technology products;
- Sound systems/security engineering principles and practices to effectively integrate information technology products into information systems;
- State-of-the-art techniques and methods for information technology product/information system assessment; and
- Comprehensive system security planning and life cycle management.[22]

[17] An organization typically exercises managerial, operational, and/or financial control over its information systems and the security provided to those systems, including the authority and capability to implement or require the security controls deemed necessary by the organization to protect organizational operations and assets, individuals, other organizations, and the Nation.

[18] See FIPS Publication 200, footnote 7.

[19] Risk assessments can be accomplished in a variety of ways depending on the specific needs of an organization. NIST Special Publication 800-30 provides guidance on the assessment of risk as part of an overall risk management process.

[20] Considerations for potential national-level impacts and impacts to other organizations in categorizing organizational information systems derive from the USA PATRIOT Act and Homeland Security Presidential Directives.

[21] The authorizing official or designated representative, by accepting the security plan, agrees to the set of security controls proposed to meet the security requirements for the information system.

[22] NIST Special Publication 800-64 provides guidance on security considerations in life cycle management.

From a systems engineering viewpoint, security is just one of many required operational capabilities for an information system supporting organizational mission/business processes—capabilities that must be funded by the organization throughout the life cycle of the system in order to achieve mission/business success. It is important that the organization *realistically* assesses the risk to organizational operations and assets, individuals, other organizations, and the Nation that arises by placing the information system into operation or continuing its operation.

In addition, information security requirements for organizational information systems must be satisfied with full consideration of the risk management strategy[23] of the organization, in light of the potential cost, schedule, and performance issues associated with the acquisition, deployment, and operation of the information system.

1.5 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with security control selection and specification including: (i) the structural components of security controls and how the controls are organized into families; (ii) security control baselines; (iii) the use of common security controls in support of organization-wide information security programs; (iv) security controls in external environments; (v) assurance in the effectiveness of security controls; and (vi) the commitment to maintain currency of the individual security controls and the control baselines.
- **Chapter Three** describes the process of selecting and specifying security controls for an information system including: (i) applying the organization’s overall approach to managing risk; (ii) categorizing the information system and determining the system impact level in accordance with FIPS 199 and FIPS 200, respectively; (iii) selecting the initial set of baseline security controls, tailoring the baseline controls, and supplementing the tailored baseline, as necessary, in accordance with an organizational assessment of risk; and (iv) assessing the security controls as part of a comprehensive continuous monitoring process.
- **Supporting appendices** provide essential security control selection and specification-related information including: (i) general references; (ii) definitions and terms; (iii) acronyms; (iv) baseline security controls for low-impact, moderate-impact, and high-impact information systems; (v) minimum assurance requirements; (vi) a master catalog of security controls; (vii) information security program management controls; (viii) international information security standards; and (ix) the application of security controls to industrial control systems.

[23] NIST Special Publication 800-39 provides guidance on organization-wide risk management.

CHAPTER TWO

THE FUNDAMENTALS

SECURITY CONTROL STRUCTURE, ORGANIZATION, BASELINES, AND ASSURANCE

This chapter presents the fundamental concepts associated with security control selection and specification including: (i) the structure of security controls and the organization of the controls in the control catalog; (ii) security control baselines; (iii) the identification and use of common security controls; (iv) security controls in external environments; (v) security control assurance; and (vi) future revisions to the security controls, the control catalog, and baseline controls.

2.1 SECURITY CONTROL ORGANIZATION AND STRUCTURE

Security controls described in this publication have a well-defined organization and structure. For ease of use in the security control selection and specification process, controls are organized into seventeen *families*.[24] Each security control family contains security controls related to the security functionality of the family. A two-character identifier is assigned to uniquely identify each security control family. In addition, there are three general classes of security controls: management, operational, and technical.[25] Table 1-1 summarizes the classes and families in the security control catalog and the associated security control family identifiers.

TABLE 1-1: SECURITY CONTROL CLASSES, FAMILIES, AND IDENTIFIERS

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

[24] Of the eighteen security control families in NIST Special Publication 800-53, seventeen families are described in the security control catalog in Appendix F, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS 200. One additional family (Program Management [PM] family) in Appendix G provides controls for information security programs. This family, while not referenced in FIPS 200, provides security controls at the organizational rather than the information-system level.

[25] A control *family* is associated with a given *class* based on the dominant characteristics of the controls in that family.

To identify each security control, a numeric identifier is appended to the family identifier to indicate the number of the control within the family. For example, CP-9 is the ninth control in the Contingency Planning family and AC-2 is the second control in the Access Control family.

The security control structure consists of the following components: (i) a *control* section; (ii) a *supplemental guidance* section; (iii) a *control enhancements* section; (iv) a *references* section; and (v) a *priority* and *baseline allocation* section. The following example from the Auditing and Accountability family illustrates the structure of a typical security control.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage of maximum audit record storage capacity*].

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects; delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

The control section provides a concise statement of the specific security capabilities needed to protect a particular aspect of an information system.[26] The control statement describes specific security-related activities or actions to be carried out by the organization or by the information system. For some security controls in the control catalog, a degree of flexibility is provided by allowing organizations to selectively define input values for certain parameters associated with the controls. This flexibility is achieved through the use of *assignment* and *selection* operations within the control (see Section 3.3). Assignment and selection operations provide an opportunity for an organization to tailor the security controls to support specific mission, business, or operational needs. For example, an organization can specify the actions to be taken by the information system in the event of an audit processing failure (see AU-5 example above), the specific events to be audited within the system, the frequency of conducting system backups, restrictions on password use, or the distribution list for organizational policies and procedures.[27]

[26] Security controls are generally designed to be *technology* and *implementation* independent and therefore, do not contain specific requirements in these areas. Organizations provide such requirements as deemed necessary in the security plan for the information system.

[27] The organization determines whether a specific assignment or selection operation is completed at the organizational level, information system level, or a combination of the two.

Once specified, the organization-defined values become part of the control, and the control implementation is assessed against the completed control statement. Selection statements narrow the potential input values by providing a specific list of items from which the organization must choose.

The supplemental guidance[28] section provides additional information related to a specific security control, but contains no requirements. Organizations are expected to apply the supplemental guidance as appropriate, when defining, developing, and implementing security controls. The supplemental guidance provides important considerations for implementing security controls in the context of an organization's operational environment, mission requirements, or assessment of risk. Security control enhancements may also contain supplemental guidance. Enhancement supplemental guidance is used in situations where the guidance is not generally applicable to the entire control but instead focused on the particular control enhancement.

The security control enhancements section provides statements of security capability to: (i) build in additional functionality to a control; and/or (ii) increase the strength of a control. In both cases, the control enhancements are used in an information system requiring greater protection due to the potential impact of loss or when organizations seek additions to the basic control functionality based on the results of a risk assessment. Control enhancements are numbered sequentially within each control so that the enhancements can be easily identified when selected to supplement the basic control. In the previous example for AU-5, if the first three control enhancements are selected, the control designation becomes AU-5 (1) (2) (3).[29] The numerical designation of a security control enhancement is used only to identify a particular enhancement within the control structure. The designation is neither indicative of the relative strength of the control enhancement nor assumes any hierarchical relationship among the enhancements.

The references section[30] includes a list of applicable federal laws, Executive Orders, directives, policies, standards, and guidelines (e.g., OMB Circulars, FIPS, and NIST Special Publications), that are relevant to a particular security control or control enhancement.[31] The references provide appropriate federal legislative and policy mandates as well as supporting information for the implementation of specific management, operational, or technical controls/enhancements. The references section also contains pertinent websites for organizations to use in obtaining additional information with regard to security control implementation and assessment.

The priority and baseline allocation section provides: (i) the recommended priority codes used for sequencing decisions during security control implementation (see Appendix D); and (ii) the initial allocation of security controls and control enhancements for low-impact, moderate-impact, and high-impact information systems (see Appendix F).

[28] The supplemental guidance section may contain information on *related controls* (i.e., security controls that either directly impact or support the control). For example, AC-6 (Least Privilege) is a related control to AC-3 (Access Control Enforcement) because AC-6 is a source for some of the authorizations to be enforced by AC-3.

[29] AU-5 Enhancement (3) is an example of a requirement in the security control catalog (Appendix F) that is *not* in any of the control baselines (Appendix D). Such requirements can be used by organizations in *supplementing* the tailored baselines as described in Section 3.3 in order to achieve what the organization deems to be adequate risk mitigation.

[30] Publications listed in the *References* section of security controls refer to the most recent versions of the publications. Organizations confirm from the respective official sources of the publications (e.g., OMB, NIST, NARA), that the most recent versions are being used for organizational application.

[31] The references listed in the security control *references section* are provided to assist organizations in applying the controls and are not intended to be inclusive or complete.

2.2 SECURITY CONTROL BASELINES

Organizations are required to adequately mitigate the risk arising from use of information and information systems in the execution of missions and business functions. A significant challenge for organizations is to determine the appropriate set of security controls, which if implemented and determined to be effective, would most cost-effectively mitigate risk while complying with the security requirements defined by applicable federal laws, Executive Orders, directives, policies, standards, or regulations (e.g., FISMA, OMB Circular A-130). Selecting the appropriate set of security controls to adequately mitigate risk by meeting the specific, and sometimes unique, security requirements of an organization is an important task—a task that clearly demonstrates the organization's commitment to security and the due diligence exercised in protecting the confidentiality, integrity, and availability of organizational information and information systems.

To assist organizations in making the appropriate selection of security controls for an information system, the concept of *baseline* controls is introduced. Baseline controls are the starting point for the security control selection process described in this document and are chosen based on the security category and associated impact level of the information system determined in accordance with FIPS 199 and FIPS 200, respectively. The tailored security control baseline (i.e., the appropriate control baseline from Appendix D adjusted in accordance with the guidance in Section 3.3) is the minimum set of security controls for the information system. Because the baseline is intended to be a broadly applicable starting point, supplements to the tailored baseline (see Section 3.3) will likely be necessary in order to achieve adequate risk mitigation. The tailored security control baseline is supplemented based on an organizational assessment of risk and the resulting controls documented in the security plan for the information system.

Appendix D provides a listing of baseline security controls. Three sets of baseline controls have been identified corresponding to the low-impact, moderate-impact, and high-impact information-system levels defined in FIPS 200 and used in Section 3.2 of this document to provide an initial set of security controls for each impact level.[32] Appendix F provides a detailed catalog of security controls for information systems, arranged by control families. Chapter Three provides additional information on how to use FIPS 199 security categories and FIPS 200 impact levels in applying the tailoring guidance to the baseline security controls and supplementing the tailored baseline in order to achieve adequate risk mitigation.

Implementation Tip

There are additional security controls and control enhancements that appear in the security control catalog (Appendix F) that are found in only higher-impact baselines or not used in any of the baselines. These additional security controls and control enhancements for the information system are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used to strengthen the level of protection provided in lower-level baselines, if deemed appropriate. At the end of the security control selection process, the agreed-upon set of controls in the security plan must be sufficient to adequately mitigate risks to organizational operations and assets, individuals, other organizations, and the Nation.

[32] The baseline security controls contained in Appendix D are not necessarily absolutes in that the tailoring guidance described in Section 3.3 provides organizations with the ability to eliminate certain controls or specify compensating controls in accordance with the terms and conditions established by authorizing officials.

2.3 COMMON CONTROLS

Common controls are security controls that are *inheritable* by one or more organizational information systems.[33] The organization assigns responsibility for common controls to appropriate organizational officials and coordinates the development, implementation, assessment, authorization, and monitoring of the controls.[34] The identification of common controls is most effectively accomplished as an organization-wide exercise with the active involvement of the chief information officer, senior information security officer, risk executive (function), authorizing officials, information system owners, information owners/stewards, and information system security officers. The organization-wide exercise considers the security categories and associated impact levels of the information systems within the organization in accordance with FIPS 199 and FIPS 200, as well as the security controls necessary to adequately mitigate the risks arising from the use of those systems (see *baseline* security controls in Section 2.2).[35] For example, common controls can be identified for all low-impact information systems by considering the associated baseline security controls in Appendix D. Similar exercises can be conducted for moderate-impact and high-impact information systems as well. When common controls protect multiple organizational information systems of differing impact levels, the controls are implemented with regard to the highest impact level among the systems.

Many of the security controls needed to protect organizational information systems (e.g., contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls) are excellent candidates for common control status. Information security program management controls (see Appendix G, PM family) may also be deemed common controls by the organization since the controls are employed at the organization level and typically serve multiple information systems. By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of common controls, security costs can be amortized across multiple information systems.

Common controls are generally documented in the organization-wide *information security program plan* unless implemented as part of a specific information system, in which case the controls are documented in the security plan for that system.[36] Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing the common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that

[33] A security control is *inheritable* by an information system or application when that system or application receives protection from the security control (or portions of the security control) and the control is developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application—entities either internal or external to the organization where the system or application resides.

[34] The Chief Information Officer, Senior Information Security Officer, or other designated organizational officials at the senior leadership level assign responsibility for the development, implementation, assessment, authorization, and monitoring of common controls to appropriate entities (either internal or external to the organization). Organizational entities assigned responsibility for common controls use the Risk Management Framework described in Chapter Three to help ensure appropriate security capabilities are provided.

[35] Each common control identified by the organization is reviewed for applicability to each specific organizational information system.

[36] Information security program plans are described in Appendix G.

the Facilities Management Office develop, implement, assess, authorize, and continuously monitor physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple systems. When common controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing boundary protection inherited by one or more organizational information systems), the information security program plan indicates which separate security plan contains a description of the common controls.

Security controls not designated as common controls are considered *system-specific controls* or *hybrid controls*. System-specific controls are the primary responsibility of information system owners and their respective authorizing officials. Organizations assign a *hybrid* status to a security control when one part of the control is deemed to be common and another part of the control is deemed to be system-specific. For example, an organization may implement the Incident Response Policy and Procedures security control (IR-1) as a hybrid control with the policy portion of the control deemed to be common and the procedures portion of the control deemed to be system-specific. Hybrid controls may also serve as templates for further control refinement. An organization may choose, for example, to implement the Contingency Planning security control (CP-2) as a template for a generalized contingency plan for all organizational information systems with individual information system owners tailoring the plan, where appropriate, for system-specific uses. Partitioning security controls into common, hybrid, and system-specific controls can result in significant savings to the organization in implementation and assessment costs as well as a more consistent application of the security controls across the organization. While the concept of security control partitioning into common, hybrid, and system-specific controls is straightforward and intuitive, the application within an organization takes significant planning and coordination.

Security plans for individual information systems identify which security controls required for those systems have been designated by the organization as common controls and which controls have been designated as system-specific or hybrid controls. Information system owners are responsible for any system-specific implementation details associated with an organization’s common controls. These implementation details are identified and described in the security plans for the individual information systems. The senior information security officer for the organization coordinates with *common control providers* (e.g., facilities/site manager, human resources manager, intrusion detection system owner) to ensure that the required controls are developed, implemented, and assessed for effectiveness. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization.

Common controls, whether employed in an information system or in the environment of operation, are authorized by a senior organizational official[37] with at least the same level of authority and responsibility for managing risk as the authorization officials for information systems inheriting the controls.[38] Authorization results relating to common controls are shared with the appropriate information system owners. A plan of action and milestones is developed and maintained for the common controls that are deemed through assessment to be less than effective. Common controls are subject to the same continuous monitoring requirements as system-specific security controls employed in individual organizational information systems.

[37] The authorizing official role, whether applied to information systems or common controls, has inherent U.S. Government authority and is assigned to government personnel only.

[38] When common controls are inherited from external environments, organizations should consult Section 2.4.

Implementation Tip

The selection of common controls is most effectively accomplished on an organization-wide basis with the involvement of the organization's senior leadership (i.e., authorizing officials, chief information officer, senior information security officer, information system owners, mission/business owners, information owners/stewards, risk executive [function]). These individuals have the collective corporate knowledge to understand the organization's priorities, the importance of the organization's operations and assets, and the relative importance of the organizational information systems that support those operations and assets. The organization's senior leaders are also in the best position to select the common controls for each security control baseline and assign organizational responsibilities for developing, implementing, assessing, authorizing, and monitoring those controls.

2.4 SECURITY CONTROLS IN EXTERNAL ENVIRONMENTS

Organizations are becoming increasingly reliant on information system services provided by external providers to carry out important missions and business functions. External information system services are services implemented outside of the authorization boundaries established by the organization for its information systems. These external services may be used by, but are not part of, organizational information systems. In some situations, external information system services may completely replace the functionality of internal information systems. Organizations are responsible and accountable for the *risk* incurred by use of services provided by external providers and address this risk by implementing compensating controls when the risk is greater than the authorizing official or the organization is willing to accept.

Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of information system security. These challenges include:

- Defining the types of external services provided to the organization;
- Describing how the external services are protected in accordance with the security requirements of the organization; and
- Obtaining the necessary assurances that the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable.

FISMA and OMB policy require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies. Security requirements for external providers including the security controls for information systems processing, storing, or transmitting federal information are expressed in appropriate contracts or other formal agreements using the Risk Management Framework and associated NIST security standards and guidelines described in Chapter Three. Organizations can require external providers to implement all steps in the Risk Management Framework described in Chapter Three with the exception of the security authorization step, which remains an inherent federal responsibility that is directly linked to the management of risk related to the use of external information system services.[39]

[39] See Implementation Tip in Section 3.3 for applying the Risk management Framework to external service providers.

The assurance or confidence that the risk from using external services is at an acceptable level depends on the trust[40] that the organization places in the external service provider. In some cases, the level of trust is based on the amount of direct control the organization is able to exert on the external service provider with regard to employment of security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls. The level of control is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider) to very limited (e.g., using a contract or service-level agreement to obtain commodity services[41] such as commercial telecommunications services). In other cases, the level of trust is based on factors that convince the organization that the requisite security controls have been employed and that a credible determination of control effectiveness exists. For example, a separately authorized external information system service provided to an organization through a well-established line of business relationship may provide a degree of trust in the external service within the tolerable risk range of the authorizing official.

The provision of services by external providers may result in some services without explicit agreements between the organization and the external entities responsible for the services. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements, etc.), the organization develops such agreements and requires the use of the security controls in Special Publication 800-53. When the organization is not in a position to require explicit agreements with external providers (e.g., the service is imposed on the organization or the service is commodity service), the organization establishes explicit assumptions about the service capabilities with regard to security.[42] Contracts between the organization and external providers may also require the active participation of the organization. For example, the organization may be required by the contract to install public key encryption-enabled client software recommended by the service provider.

Ultimately, the responsibility for adequately mitigating unacceptable risks arising from the use of external information system services remains with the authorizing official. Organizations require that an appropriate *chain of trust* be established with external service providers when dealing with the many issues associated with information system security. A chain of trust requires that the

[40] The level of trust that an organization places in an external service provider can vary widely, ranging from those who are highly trusted (e.g., business partners in a joint venture that share a common business model and common goals) to those who are less trusted and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

[41] Commercial providers of commodity-type services typically organize their business models and services around the concept of shared resources and devices for a broad and diverse customer base. Therefore, unless organizations obtain fully dedicated services from commercial service providers, there may be a need for greater reliance on compensating security controls to provide the necessary protections for the information system that relies on those external services. The organization’s risk assessment and risk mitigation activities reflect this situation.

[42] In situations where an organization is procuring information system services or technologies through a centralized acquisition vehicle (e.g., governmentwide contract by the General Services Administration or other preferred and/or mandatory acquisition organization), it may be more efficient and cost-effective for the originator of the contract to establish and maintain a stated level of trust with the external provider (including the definition of required security controls and level of assurance with regard to the provision of such controls). Organizations subsequently acquiring information system services or technologies from the centralized contract can take advantage of the negotiated trust level established by the procurement originator and thus avoid costly repetition of the activities necessary to establish such trust. For example, a procurement originator could authorize an information system providing external services to the federal government under specific terms and conditions of the contract. A federal agency requesting information system services under the terms of the contract would not be required to reauthorize the information system when acquiring such services (unless the request included services outside the scope of the original contract).

organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The chain of trust can be complicated due to the number of entities participating in the consumer-provider relationship and the type of relationship between the parties. External service providers may also in turn outsource the services to other external entities, making the chain of trust even more complicated and difficult to manage. Depending on the nature of the service, it may simply be unwise for the organization to place significant trust in the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating controls or accepts a greater degree of risk.

2.5 SECURITY CONTROL ASSURANCE

Assurance is the grounds for confidence that the security controls implemented within an information system are effective in their application. Assurance can be obtained in a variety of ways including:

- Actions taken by developers, implementers, and operators in the specification, design, development, implementation, operation, and maintenance of security controls;[43] and
- Actions taken by security control assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Appendix E describes the minimum assurance requirements[44] for security controls in low-impact, moderate-impact, and high-impact information systems. For security controls in low-impact systems, the emphasis is on the control being in place with the expectation that no obvious errors exist and that as flaws are discovered, they are addressed in a timely manner. For security controls in moderate-impact systems, in addition to the assurance requirements for low-impact systems, the emphasis is on increasing the grounds for confidence in control correctness. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer or control implementer incorporates, as part of the control, specific capabilities to increase grounds for confidence that the control meets its function or purpose. For security controls in high-impact systems, in addition to the assurance requirements for moderate-impact systems, the emphasis is on requiring within the control, the capabilities that are needed to support ongoing, consistent operation of the control and to support continuous improvement in the control's effectiveness. There are additional assurance requirements available to developers/implementers of security controls supplementing the minimum assurance requirements for the moderate-impact and high-impact information systems in order to protect against threats from highly skilled, highly motivated, and well-resourced threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

[43] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls. This may include in addition to organizational personnel, for example, hardware and software vendors providing the security controls and contractors implementing the controls.

[44] Assurance requirements imposed upon developers and implementers of security controls are addressed in this special publication. Assurance gained from the assessment of security controls (e.g., by testers, evaluators, auditors, Inspectors General, information system owners) is addressed in NIST Special Publication 800-53A.

2.6 REVISIONS AND EXTENSIONS

The set of security controls listed in this publication represents the current state-of-the-practice safeguards and countermeasures for federal information systems and organizations. The security controls will be carefully reviewed and revised periodically to reflect:

- Experience gained from using the controls;
- Changing security requirements;
- Emerging threats, vulnerabilities, and attack methods; and
- Availability of new technologies.[45]

The security controls in the security control catalog are expected to change over time, as controls are withdrawn, revised, and added. The security controls defined in the low, moderate, and high baselines are also expected to change over time as the level of security and due diligence for mitigating risks within organizations changes. In addition to the need for change, the need for stability will be addressed by requiring that proposed additions, deletions, or modifications to the catalog of security controls go through a rigorous public review process to obtain government and private sector feedback and to build consensus for the changes. A stable, yet flexible and technically rigorous set of security controls will be maintained in the security control catalog.

[45] The security control catalog in Appendix F will be updated as needed with new controls developed from national-level threat databases containing information on known cyber attacks. The proposed modifications to security controls and security control baselines will be carefully weighed with each revision cycle, considering the desire for stability on one hand, and the need to respond to changing threats and vulnerabilities, new attack methods, new technologies, and the important objective of raising the foundational level of security over time. Organizations may develop new controls when appropriate controls are not available in Appendix F.

CHAPTER THREE

THE PROCESS

SELECTION AND SPECIFICATION OF SECURITY CONTROLS

This chapter describes the process of selecting and specifying security controls for an organizational information system to include: (i) applying the organization's approach to managing risk; (ii) categorizing the information system and determining the system impact level in accordance with FIPS 199 and FIPS 200, respectively; (iii) selecting security controls, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk; and (iv) assessing the security controls as part of a comprehensive continuous monitoring process.

3.1 MANAGING RISK

The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program for the management of risk—that is, the risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation of an information system. The management of risk is a key element in the organization's information security program and provides an effective framework for selecting the appropriate security controls for an information system—the security controls necessary to protect individuals and the operations and assets of the organization. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations, standards, or guidelines. The following activities related to managing risk, included as part of the *Risk Management Framework*, are paramount to an effective information security program and can be applied to both new and legacy information systems within the context of the Federal Enterprise Architecture and system development life cycle—

- ***Categorize*** the information system and the information processed, stored, and transmitted by that system based on a FIPS 199 impact analysis.
- ***Select*** an initial set of baseline security controls for the information system based on the system impact level and minimum security requirements defined in FIPS 200; apply tailoring guidance;[46] supplement the tailored baseline security controls based on an organizational assessment of risk[47] and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances; and specify assurance requirements.
- ***Implement*** the security controls and describe how the controls are employed within the information system and its environment of operation.[48]
- ***Assess*** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.[49]

[46] Tailoring guidance provides organizations with specific considerations on the applicability and implementation of individual security controls in the control baselines (see Section 3.3).

[47] NIST Special Publication 800-30 provides guidance on the assessment of risk.

[48] For legacy systems, some or all of the security controls selected may already be implemented.

[49] NIST Special Publication 800-53A provides guidance on assessing the effectiveness of security controls.

- ***Authorize*** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.[50]
- ***Monitor*** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Figure 3-1 illustrates the specific activities in the Risk Management Framework and the information security standards and guidance documents associated with each activity.[51] The remainder of this chapter focuses on several key activities in the Risk Management Framework associated with security control selection and specification.

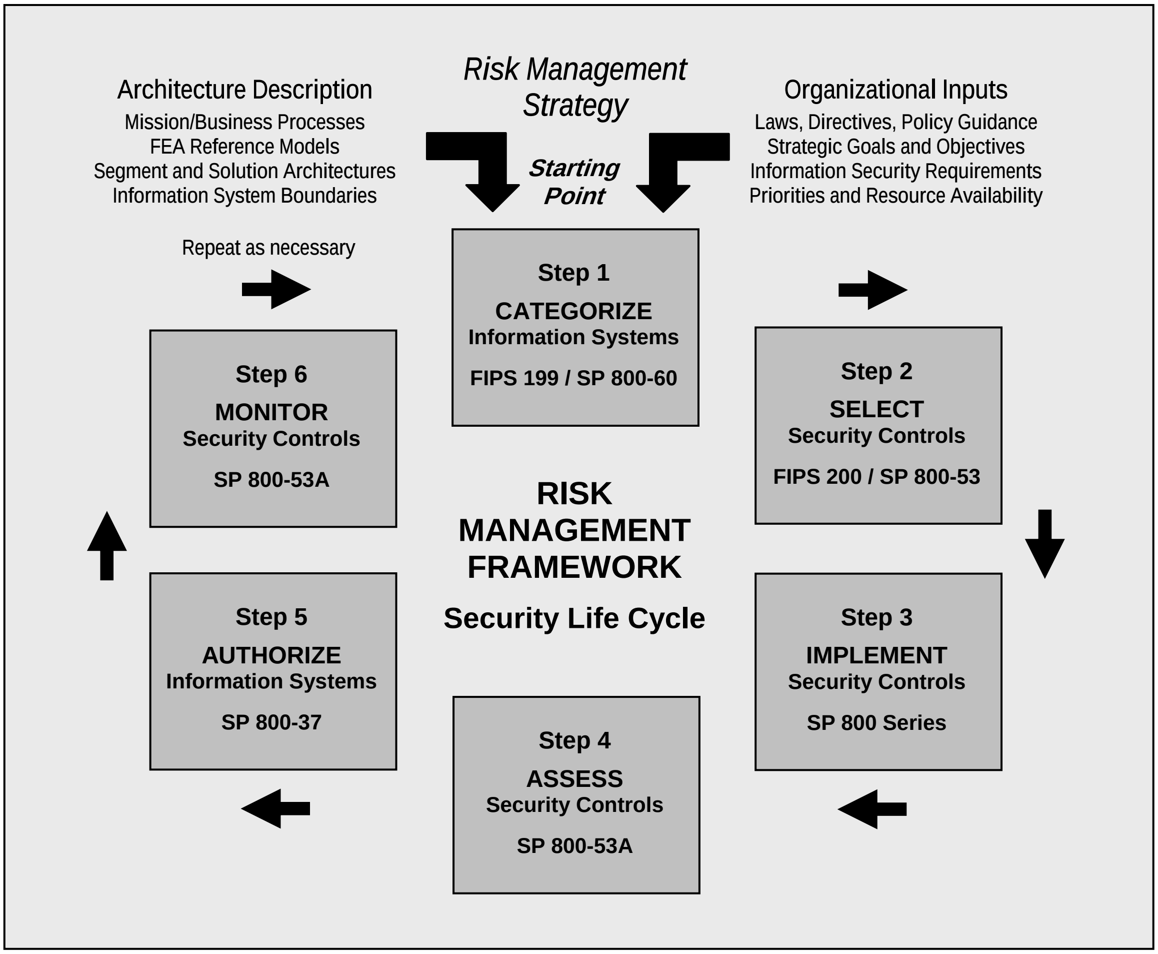


FIGURE 3-1: RISK MANAGEMENT FRAMEWORK

[50] NIST Special Publication 800-37 provides guidance on the security authorization of information systems.

[51] NIST Special Publication 800-39 provides guidance on organization-wide risk management including the development of risk management strategies, risk-related governance issues, defining protection requirements and associated risks for organizational mission/business processes, integration of security and privacy requirements into enterprise architectures, and managing risk within the system development life cycle.

3.2 CATEGORIZING THE INFORMATION SYSTEM

FIPS 199, the mandatory security categorization standard, is predicated on a simple and well-established concept—determining appropriate security priorities for organizational information systems and subsequently applying appropriate measures to adequately protect those systems. The security controls applied to a particular information system are commensurate with the potential adverse impact on organizational operations, organizational assets, individuals, other organizations, and the Nation should there be a loss of confidentiality, integrity, or availability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability (RMF Step 1). The potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each type of information processed, stored, or transmitted by those information systems.[52] The generalized format for expressing the security category (SC) of an information system is:

$$\textbf{SC}_{\text{information system}} = \{(\textbf{confidentiality}, \textit{impact}), (\textbf{integrity}, \textit{impact}), (\textbf{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are low, moderate, or high.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept is introduced in FIPS 200 to determine the impact level of the information system for the express purpose of selecting an initial set of security controls from one of the three security control baselines.[53] Thus, a *low-impact* system is defined as an information system in which all three of the security objectives are low. A *moderate-impact* system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact* system is an information system in which at least one security objective is high.

Implementation Tip

To determine the overall impact level of the information system:

- First, determine the different types of information that are processed, stored, or transmitted by the information system (e.g., financial sector oversight, inspections and auditing, official information dissemination, etc.). NIST Special Publication 800-60 provides guidance on a variety of information types commonly used by organizations.
- Second, using the impact levels in FIPS 199 and the recommendations of NIST Special Publication 800-60, categorize the confidentiality, integrity, and availability of each information type.
- Third, determine the information system security categorization, that is, the highest impact level for each security objective (confidentiality, integrity, availability) from among the categorizations for the information types associated with the information system.
- Fourth, determine the overall impact level of the information system from the highest impact level among the three security objectives in the system security categorization.

[52] NIST Special Publication 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance on the assignment of security categories to information systems.

[53] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well. Accordingly, the security controls in the control catalog are not categorized by security objective—rather, they are grouped into baselines to provide a general protection capability for classes of information systems based on impact level. The application of scoping guidance may allow selective security control baseline tailoring based on the individual impact levels for confidentiality, integrity, and availability (see Section 3.3).

3.3 SELECTING SECURITY CONTROLS

Once the impact level of the information system is determined, the organization begins the security control selection process (RMF Step 2). There are three steps in the control selection process carried out sequentially: (i) *selecting* the initial set of baseline security controls; (ii) *tailoring* the baseline security controls; and (iii) *supplementing* the tailored baseline. The following sections describe each of these steps in greater detail.[54]

Selecting the Initial Baseline Security Controls

The first step in selecting security controls for the information system is to choose the appropriate set of baseline controls. The selection of the initial set of baseline security controls is based on the impact level of the information system as determined by the security categorization process described in Section 3.2. The organization selects one of three sets of baseline security controls from Appendix D corresponding to the low-impact, moderate-impact, or high-impact rating of the information system. Note that not all security controls are assigned to baselines, as indicated by the phrase *not selected*. Similarly, not all control enhancements are assigned to baselines, as indicated by the security control being *not selected* or the enhancement number enclosed in parenthesis, not appearing in any baseline.

Tailoring the Baseline Security Controls

After selecting the initial set of baseline security controls from Appendix D, the organization initiates the tailoring process to appropriately modify and more closely align the controls with the specific conditions within the organization (i.e., conditions specific to the information system or its environment of operation). The tailoring process includes:

- Applying *scoping guidance* to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline;
- Selecting (or specifying) *compensating security controls*, if needed, to adjust the preliminary set of controls to obtain an equivalent set deemed to be more feasible to implement; and
- Specifying *organization-defined parameters* in the security controls via explicit assignment and selection statements to complete the definition of the tailored baseline.

To achieve a cost-effective, risk-based approach to providing adequate information security organization-wide, the baseline tailoring activities are coordinated with and approved by appropriate organizational officials (e.g., authorizing officials, authorizing official designated representatives, risk executive (function), chief information officers, or senior information security officers) prior to implementing the security controls. Organizations have the flexibility to perform the tailoring process at the organization level for all information systems (either as the required tailored baseline or as the starting point for system-specific tailoring), at the individual information system level, or using a combination of organization-level and system-specific approaches. Tailoring decisions for all affected security controls in the selected baseline, including the specific rationale for those decisions, are documented in the security plan for the information system and approved by appropriate organizational officials as part of the security plan approval process.[55]

[54] The general security control selection process may be augmented or further detailed by additional sector-specific guidance such as that provided for industrial control systems in Appendix I.

[55] The level of detail required in documenting tailoring decisions in the security control selection process is strictly at the discretion of the organization and is consistent with the impact level of the information system.

Scoping Guidance

Scoping guidance provides organizations with specific terms and conditions on the applicability and implementation of individual security controls in the security control baselines. Application of scoping guidance helps to ensure that organizations implement *only* those controls that are essential to providing the appropriate level of protection for the information system based on specific mission/business requirements and particular environments of operation. There are several scoping considerations described below, that can potentially affect how the baseline security controls are applied and implemented by organizations:

- COMMON CONTROL-RELATED CONSIDERATIONS—

  Security controls designated by the organization as common controls are, in most cases, managed by an organizational entity other than the information system owner. Organizational decisions on which security controls are viewed as common controls may greatly affect the responsibilities of individual information system owners with regard to the implementation of controls in a particular baseline. Every security control in the tailored and supplemented set of controls for an information system is identified in the security plan as a common, system-specific, or hybrid control (see Section 2.3).

- SECURITY OBJECTIVE-RELATED CONSIDERATIONS—

  Security controls that support only one or two of the confidentiality, integrity, or availability security objectives may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if not defined in a lower baseline) if, and only if, the downgrading action: (i) is consistent with the FIPS 199 security category for the supported security objective(s) before moving to the FIPS 200 impact level (i.e., high water mark);[56] (ii) is supported by an organizational assessment of risk; and (iii) does not adversely affect the level of protection for the security-relevant information within the information system.[57] The following security controls are recommended candidates for downgrading: (i) confidentiality [MA-3 (3), MP-2 (1), MP-3, MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9]; (ii) integrity [SC-8]; and (iii) availability [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6].[58]

[56] When applying the “high water mark” process in Section 3.2, some of the original FIPS 199 confidentiality, integrity, or availability security objectives may have been upgraded to a higher baseline of security controls. As part of this process, security controls that uniquely support the confidentiality, integrity, or availability security objectives may have been upgraded unnecessarily. Consequently, it is recommended that organizations consider appropriate and allowable downgrading actions to ensure cost-effective, risk-based application of security controls.

[57] Information that is security-relevant at the system level (e.g., password files, network routing tables, cryptographic key management information) is distinguished from user-level information within an information system. Certain security controls within an information system are used to support the security objectives of confidentiality and integrity for both user-level and system-level information. Caution should be exercised in downgrading confidentiality or integrity-related security controls to ensure that the downgrading action does not result in insufficient protection for the security-relevant information within the information system. Security-relevant information must be protected at the high water mark in order to achieve that level of protection for any of the security objectives related to user-level information.

[58] Downgrading actions apply only to the moderate and high baselines. Certain security controls that are uniquely attributable to confidentiality, integrity, or availability that would ordinarily be considered as potential candidates for downgrading (e.g., AC-16, AU-10, IA-7, PE-12, PE-14, PL-5, SC-5, SC-13, SC-14, SC-16) are eliminated from consideration because the controls are either selected for use in all baselines and have no enhancements that could be downgraded, or the controls are optional and not selected for use in any baseline. Organizations should exercise caution when considering downgrading security controls that do not appear in the list in Section 3.3 to ensure that the downgrading action does not affect security objectives other than the objectives targeted for downgrading.

- SYSTEM COMPONENT ALLOCATION-RELATED CONSIDERATIONS—

  Security controls in the baseline represent an information system-wide set of controls that may not be necessary for or applicable to every component in the system. Security controls are applicable only to the components of the information system that provide or support the security capability addressed by the control and are sources of potential risk being mitigated by the control. For example, auditing controls are typically allocated to components of an information system that provide auditing capability (e.g., servers, etc.) and are not necessarily applied to every user-level workstation within the organization; or when information system components are single-user, not networked, or part of a physically isolated network, one or more of these characteristics may provide appropriate rationale for not allocating selected controls to that component. Organizations assess the inventory of information system components to determine which security controls are applicable to the various components and subsequently make explicit decisions regarding where to allocate the controls in order to satisfy organizational security requirements.[59]

- TECHNOLOGY-RELATED CONSIDERATIONS—

  Security controls that refer to specific technologies (e.g., wireless, cryptography, public key infrastructure) are applicable only if those technologies are employed or are required to be employed within the information system. Security controls that can be supported by automated mechanisms do not require the development of such mechanisms if the mechanisms do not already exist or are not readily available in commercial or government off-the-shelf products. For example, automated mechanisms may be used to maintain up-to-date, complete, accurate, and readily available baseline configurations of organizational information systems. If automated mechanisms are not readily available, cost-effective, or technically feasible, compensating security controls, implemented through nonautomated mechanisms or procedures, are used to satisfy specified security control requirements (see terms and conditions for selecting and applying compensating controls below).

- PHYSICAL INFRASTRUCTURE-RELATED CONSIDERATIONS—

  Security controls that refer to organizational facilities (e.g., physical controls such as locks and guards, environmental controls for temperature, humidity, lighting, fire, and power) are applicable only to those sections of the facilities that directly provide protection to, support for, or are related to the information system (including its information technology assets such as electronic mail or web servers, server farms, data centers, networking nodes, workstations, boundary protection devices, and communications equipment).

- POLICY/REGULATORY-RELATED CONSIDERATIONS—

  Security controls that address matters governed by applicable federal laws, Executive Orders, directives, policies, standards, or regulations (e.g., privacy impact assessments) are required only if the employment of those controls is consistent with the types of information and information systems covered by the applicable laws, Executive Orders, directives, policies, standards, or regulations.

[59] As technology advances, more powerful and diverse functionality can be found in such devices as personal digital assistants and cellular telephones. These devices may require the application of security controls in accordance with an organizational assessment of risk. While the scoping guidance may support not allocating a particular security control to a specific component, any residual risk associated with the absence of that control must be addressed to adequately protect organizational operations and assets, individuals, other organizations, and the Nation.

- OPERATIONAL/ENVIRONMENTAL-RELATED CONSIDERATIONS—

  Security controls that are based on specific assumptions about the operational environment are applicable only if the information system is employed in the assumed environment. For example, certain physical security controls may not be applicable to space-based information systems, and temperature and humidity controls may not be applicable to remote sensors that exist outside of the indoor facilities that contain information systems.

- SCALABILITY-RELATED CONSIDERATIONS—

  Security controls are scalable with regard to the extent and rigor of the implementation. Scalability is guided by the FIPS 199 security categorization and associated FIPS 200 impact level of the information system being protected. For example, a contingency plan for a high-impact information system may be quite lengthy and contain a significant amount of implementation detail. In contrast, a contingency plan for a low-impact information system may be considerably shorter and contain much less implementation detail. Organizations use discretion in applying the security controls to information systems, giving consideration to the scalability factors in particular environments. This approach facilitates a cost-effective, risk-based approach to security control implementation that expends no more resources than necessary, yet achieves sufficient risk mitigation and adequate security.

- PUBLIC ACCESS-RELATED CONSIDERATIONS—

  When public access to organizational information systems is allowed, security controls are applied with discretion since some security controls from the specified control baselines (e.g., identification and authentication, personnel security controls) may not be applicable to public access. For example, while the baseline controls require identification and authentication of organizational personnel that maintain and support information systems providing the public access services, the same controls might not be required for access to those information systems through public interfaces to obtain publicly available information. On the other hand, identification and authentication would be required for users accessing information systems through public interfaces in some instances, for example, to access/change their personal information.

Compensating Security Controls

Organizations may find it necessary on occasion, to employ compensating security controls. This may occur, for example, when an organization is unable to implement a security control in the baseline or when, due to the specific nature of an information system or its environment of operation, the control in the baseline is not a cost-effective means of obtaining the needed risk mitigation. A compensating security control is a management, operational, or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines described in Appendix D, that provides an equivalent or comparable level of protection for an information system and the information processed, stored, or transmitted by that system.[60] Compensating controls are typically selected after applying the scoping considerations in the tailoring guidance to the initial set of baseline security controls. For example, compensating controls may be needed by the organization when

[60] More than one compensating control may be required to provide the equivalent or comparable protection for a particular security control in NIST Special Publication 800-53. For example, an organization with significant staff limitations may compensate for the separation of duty security control by strengthening the audit, accountability, and personnel security controls within the information system. Acceptable compensating controls do not necessarily require the development of new security controls.

applying technology-based considerations addressing the lack of capability to support automated mechanisms as part of a security control or control enhancement requirement. A compensating control for an information system may be employed only under the following conditions:

- The organization selects the compensating control from NIST Special Publication 800-53, or if an appropriate compensating control is not available, the organization adopts a suitable compensating control from another source;[61]
- The organization provides supporting rationale for how the compensating control delivers an equivalent security capability for the information system and why the related baseline security control could not be employed; and
- The organization assesses and formally accepts the risk associated with employing the compensating control in the information system.

Organization-Defined Security Control Parameters

Security controls containing organization-defined parameters (i.e., assignment and/or selection operations) give organizations the flexibility to define certain portions of the controls to support specific organizational requirements or objectives (see AU-5 example in Section 2.1). After the application of scoping guidance and selection of compensating security controls, organizations review the list of security controls for assignment and selection operations and determine the appropriate organization-defined values for the identified parameters. Values for organization-defined parameters are adhered to unless more restrictive values are prescribed by applicable federal laws, Executive Orders, directives, policies, standards, guidelines, or regulations. Organizations may choose to specify values for security control parameters before selecting compensating controls since the specification of those parameters completes the definition of the security control and may affect the compensating control requirements.

Supplementing the Tailored Baseline

The tailored security control baseline is the foundation or starting point for determining the needed set of security controls for an information system. As described in Section 3.1, the final determination of the appropriate set of security controls necessary to provide adequate security for an information system is a function of the organization’s assessment of risk and what is required to sufficiently mitigate the risks to organizational operations and assets, individuals, other organizations, and the Nation.[62] In many cases, additional security controls or control enhancements will be needed to address specific threats to and vulnerabilities in an information system and to satisfy the requirements of applicable federal laws, Executive Orders, directives, policies, standards, or regulations. The risk assessment at this stage in the security control selection process provides important inputs to determine the sufficiency of the security controls in the tailored baseline. Organizations are encouraged to make maximum use of the security control catalog in Appendix F to facilitate the process of enhancing security controls and/or adding controls to the tailored baseline.[63]

[61] Organizations should make every attempt to select compensating controls from the security control catalog in NIST Special Publication 800-53. Organization-defined compensating controls are employed only as a last resort when the organization deems that the security control catalog does not contain suitable compensating controls.

[62] Considerations for potential national-level impacts and impacts to other organizations in categorizing organizational information systems derive from the USA PATRIOT Act and Homeland Security Presidential Directives.

[63] Security controls and control enhancements selected to supplement tailored baselines are allocated to appropriate information system components in the same manner as the control allocations carried out by the organization in the initial baselines. See Section 3.3, S*coping Guidance*, for security control allocation.

In selecting the security controls and control enhancements to supplement the tailored baseline, an organization can employ a *requirements definition* approach or a *gap analysis* approach. In the requirements definition approach, the organization acquires specific and credible threat[64] information (or makes a reasonable assumption) about the activities of adversaries with certain capabilities or attack potential (e.g., skill levels, expertise, available resources). To effectively withstand cyber attacks from adversaries with the stated capabilities or attack potential, the organization strives to achieve a certain level of security capability or cyber preparedness. Organizations can choose additional security controls and control enhancements from Appendix F to obtain such security capability or level of preparedness. In contrast to the requirements definition approach, the gap analysis approach begins with an organizational assessment of its current security capability or level of cyber preparedness. From that initial security capability assessment, the organization determines the types of threats it can reasonably expect to address. If the organization's current security capability or level of cyber preparedness is insufficient, the gap analysis determines the required capability and level of preparedness. The organization subsequently defines the security controls and control enhancements from Appendix F needed to achieve the desired capability or cyber preparedness level.[65]

There may be situations in which an organization is employing information technology beyond its ability to adequately protect essential missions and business functions (e.g., certain web-based, social networking, and collaborative computing-based technologies). That is, the organization cannot apply sufficient security controls within an information system to adequately reduce or mitigate risk. In those situations, an alternative strategy is needed to prevent the mission and business functions from being adversely affected; a strategy that considers the mission/business risks that result from an aggressive use of information technology. Restrictions on the types of technologies used and how the information system is employed provide an alternative method to reduce or mitigate risk when security controls cannot be implemented within technology/resource constraints, or when controls lack reasonable expectation of effectiveness against identified threat sources. Restrictions on the use of information systems and specific information technologies are in many situations, the only practical or reasonable course of action an organization can take in order to have the ability to carry out its assigned missions and business functions in the face of determined adversaries. Examples of use restrictions include:

- Limiting the information an information system can process, store, or transmit or the manner in which an organizational mission or business function is automated;
- Prohibiting external access to organizational information by removing selected information system components from the network (i.e., air gapping); and
- Prohibiting public access to moderate-impact or high-impact information systems, unless an explicit determination is made authorizing such access.

Organizations document the decisions taken during the security control selection process, providing a sound rationale for those decisions. This documentation is essential when examining the security considerations for information systems with respect to potential mission/business impact. The resulting set of security controls along with the supporting rationale for selection decisions and any information system use restrictions are documented in the security plan for the information system. Documenting in the security plan any significant risk management decisions

[64] While this example focuses on threats to information systems from purposeful attacks, the scope of concern to most organizations also includes environmental disruptions and human errors.

[65] NIST Special Publication 800-30 provides guidance on conducting risk assessments. Future updates to Special Publication 800-30 will include additional information on threat taxonomies and security capabilities.

in the security control selection process is imperative in order for authorizing officials to have the necessary information to make credible, risk-based decisions regarding the authorization of organizational information systems. In addition, without such information, the understanding, assumptions, and rationale supporting those important risk decisions will, in all likelihood, not be available when the state of the information systems or environments of operation change, and the original risk decisions are revisited.

Figure 3-2 summarizes the security control selection process,[66] including tailoring of the initial security control baseline and any additional modifications to the baseline required based on an organizational assessment of risk.[67]

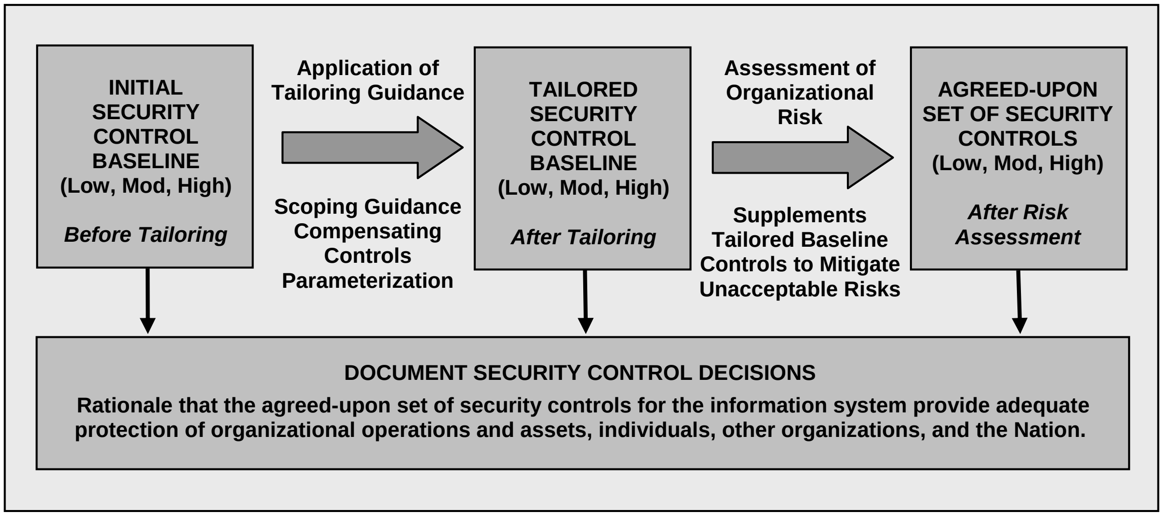

INITIAL SECURITY CONTROL BASELINE (Low, Mod, High)
Before Tailoring
Application of Tailoring Guidance
Scoping Guidance
Compensating Controls
Parameterization
TAILORED SECURITY CONTROL BASELINE (Low, Mod, High)
After Tailoring
Assessment of Organizational Risk
Supplements Tailored Baseline Controls to Mitigate Unacceptable Risks
AGREED-UPON SET OF SECURITY CONTROLS (Low, Mod, High)
After Risk Assessment
DOCUMENT SECURITY CONTROL DECISIONS
Rationale that the agreed-upon set of security controls for the information system provide adequate protection of organizational operations and assets, individuals, other organizations, and the Nation.

FIGURE 3-2: SECURITY CONTROL SELECTION PROCESS

[66] Some of the steps in the Risk Management Framework are represented by actual security controls (e.g., RA-2, *Security Categorization*, CA-2, *Security Assessment*, CA-6, *Security Authorization*, and CA-7, *Continuous Monitoring*) in Appendix F. A few other selected security controls must be implemented initially to complete the first two steps in the Risk Management Framework. For example, RA-3, Risk Assessment, is implemented to conduct an organizational assessment of risk to support selecting, tailoring, and supplementing the security control baseline. Security control PL-2, Security Plan, is implemented to document the agreed-upon security controls upon completion of the control selection process. Organizations select and implement security controls in the appropriate sequence to fully execute the steps in the Risk Management Framework.

[67] An information system can employ security controls at different layers within the system. An operating system, for example, typically provides an access control capability that includes the identification and authentication of users. An application, hosted by that operating system, may also provide its own access control capability requiring users to go through a second level of identification and authentication, thus rendering an additional level of protection for the information system. Organizations carrying out the security control selection process consider components at all layers within the information system as part of effective organizational security architecture implementing a defense-in-depth security strategy.

Implementation Tip

Many organizations own and operate large and complex information systems, sometimes referred to as a system-of-systems. System architecture plays a key part in the security control selection process for these types of information systems. Organizations can address a large and complex system by dividing the system into two or more subsystems and applying the FIPS 199 security categorization and FIPS 200 impact level determination to each subsystem. Applying separate impact levels to each subsystem does not change the overall impact level of the information system; rather, it allows the constituent subsystems to receive a separate allocation of security controls instead of deploying higher impact controls across every subsystem. It is not valid to treat the subsystems as entirely independent entities, however, since the subsystems are interdependent and interconnected. The organization develops a security architecture to allocate security controls among the subsystems including monitoring and controlling communications at key internal boundaries within the large and complex system (or system-of-systems) and provides system-wide controls that meet or exceed the highest information system impact level of the constituent subsystems inheriting the security capability from those system-wide controls.

The organization considers that replicated subsystems within a large and complex information system may exhibit common vulnerabilities that can be exploited by a common threat source; thereby negating the redundancy that might be relied upon as a risk mitigation measure. The impact due to a security incident against one constituent subsystem might cascade and impact many subsystems at the same time. Risk levels can be adjusted upward or downward based on the actual deployment of security controls, the effectiveness of the controls, the environment in which the information system is operating, and how the organization is using its information technology.

New Development and Legacy Systems

The security control selection process described in this section can be applied to organizational information systems from two different perspectives: (i) new development; and (ii) legacy. For a new development system, the security control selection process is applied from a *requirements definition* perspective since the information system does not yet exist and the organization is conducting an initial security categorization. The security controls included in the security plan for the information system serve as a security specification for the organization and are expected to be incorporated into the system during the development and implementation phases of the system development life cycle. In contrast, for a legacy information system, the security control selection process is applied from a *gap analysis* perspective when the organization is anticipating significant changes to the system (e.g., during major upgrades, modifications, or outsourcing). Since the information system already exists, the organization in all likelihood has completed the security categorization and security control selection processes resulting in the documentation of a previously agreed-upon set of security controls in the security plan and the implementation of those controls within the information system. Therefore, the gap analysis can be applied in the following manner:

- First, reconfirm or update as necessary, the FIPS 199 security category and FIPS 200 impact level for the information system based on the different types of information that are *currently* being processed, stored, or transmitted by the system.
- Second, review the existing security plan that describes the security controls that are currently employed considering any updates to the security category and information system impact level as well as any changes to the organization, the system, or the operational environment. Reassess the risk and revise the security plan as necessary, including documenting any additional security controls that *would* be needed by the system to ensure that the risk to organizational operations, organizational assets, individuals, other organizations, and the Nation, remains at an acceptable level.

- Third, *implement* the security controls described in the updated security plan, document in the plan of action and milestones any controls not implemented, and continue with the remaining steps in the Risk Management Framework in the same manner as a new development system.

Applying Gap Analyses to External Service Providers

The gap analysis perspective is also applied when interacting with external service providers. As described in Section 2.4, organizations are becoming increasingly reliant on external providers for critical information system services. Using the steps in the gap analysis described above, the organization can effectively use the acquisition process and appropriate contractual vehicles to require external providers to carry out, in collaboration with the organization, the security categorization and security control selection steps in the RMF. The resulting information can help determine what security controls the external provider either has in place or intends to implement for the information system services that are to be provided to the organization. If a security control deficit exists, the responsibility for adequately mitigating unacceptable risks arising from the use of external information system services remains with the authorizing official. In such situations, the organization can reduce the organizational risk to an acceptable level by:

- Using the existing contractual vehicle to require the external provider to meet the additional security control requirements established by the organization;
- Negotiating with the provider for additional security controls (including compensating controls) if the existing contractual vehicle does not provide for such added requirements; or
- Employing alternative risk mitigation measures[68] within the organizational information system when a contract either does not exist or the contract does not provide the necessary leverage for the organization to obtain needed security controls.

3.4 MONITORING SECURITY CONTROLS

After the security controls are implemented and assessed for effectiveness, the information system is authorized for operation in accordance with the organization’s risk management strategy (RMF Steps 3, 4, and 5). The organization subsequently initiates specific follow-on actions as part of a comprehensive continuous monitoring program. The continuous monitoring program includes an ongoing assessment of security control effectiveness to determine if there is a need to modify or update the current deployed set of security controls based on changes in the information system or its environment of operation (RMF Step 6). In particular, the organization revisits on a regular basis, the risk management activities described in the Risk Management Framework. In addition to the ongoing activities associated with the implementation of the Risk Management Framework, there are certain events which can trigger the immediate need to assess the security state of the information system and if required, modify or update the current security controls. These events include, for example:

- An incident results in a breach to the information system, producing a loss of confidence by the organization in the confidentiality, integrity, or availability of information processed, stored, or transmitted by the system;
- A newly identified, credible, information system-related threat to organizational operations and assets, individuals, other organizations, or the Nation is identified based on intelligence information, law enforcement information, or other credible sources of information;

[68] For example, local policies, procedures, and/or compensating controls could be established on the organization side to serve as alternative mitigation measures for risks identified in a gap analysis.

- Significant changes to the configuration of the information system through the removal or addition of new or upgraded hardware, software, or firmware or changes in the operational environment[69] potentially degrade the security state of the system; or
- Significant changes to the organizational risk management strategy, information security policy, supported missions and/or business functions, or information being processed, stored, or transmitted by the information system.

When such events occur, organizations, at a minimum, take the following actions:[70]

- *Reconfirm the security category and impact level of the information system.*

  The organization reexamines the FIPS 199 security category and FIPS 200 impact level of the information system to confirm that the security category and system impact level previously established and approved by the authorizing official are still valid. The resulting analysis may provide new insights as to the overall importance of the information system in allowing the organization to fulfill its mission/business responsibilities.

- *Assess the current security state of the information system and the risk to organizational operations and assets, individuals, other organizations, and the Nation.*

  The organization investigates the information system vulnerability (or vulnerabilities) exploited by the threat source (or potentially exploitable by a threat source) and the security controls currently implemented within the system as described in the security plan. The exploitation of information system vulnerabilities by a threat source may be traced to one or more factors including but not limited to: (i) the failure of currently implemented security controls; (ii) missing security controls; (iii) insufficient strength of security controls; and/or (iv) an increase in the capability of the threat source. Using the results from the assessment of the current security state, the organization reassesses the risks arising from use of the information system.

- *Plan for and initiate any necessary corrective actions.*

  Based on the results of an updated risk assessment, the organization determines what additional security controls and/or control enhancements or corrective actions for existing controls are necessary to adequately mitigate risk. The security plan for the information system is updated to reflect any initial changes to the original plan. A plan of action and milestones is developed for any noted weaknesses or deficiencies that are not immediately corrected and for the implementation of any security control upgrades or additional controls. After the security controls and/or control upgrades have been implemented and any other weaknesses or deficiencies corrected, the controls are assessed for effectiveness to determine if the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. If necessary, the security plan is updated to reflect any additional corrective actions taken by the organization to mitigate risk.

[69] Examples of significant changes in the operational environment are interconnection of external information systems and large increases or decreases in the size of the community of users accessing the information system.

[70] Organizations determine the specific types of events that would trigger changes to the security controls within the information system or its environment of operation and a resulting modification to the security plan. The decision to commit resources in light of such events is guided by an organizational assessment of risk.

- *Consider reauthorizing the information system.*

  Depending on the severity of the event, the adverse impact on organizational operations and assets, individuals, other organizations, and the Nation, and the extent of the corrective actions required to fix the identified weaknesses or deficiencies in the information system, the organization may need to consider reauthorizing the information system in accordance with the provisions of NIST Special Publication 800-37. The authorizing official makes the final determination on the need to reauthorize the information system in consultation with the risk executive (function), system and mission/business owners, the senior information security officer, and the chief information officer. The authorizing official may choose to conduct a limited reauthorization focusing *only* on the affected components of the information system and the associated security controls and/or control enhancements which have been changed during the update. Authorizing officials have sufficient information available from security control assessments to initiate, with an appropriate degree of confidence, necessary corrective actions.

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, REGULATIONS, MEMORANDA, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.
4. USA PATRIOT Act (P.L. 107-56), October 2001.
5. Privacy Act of 1974 (P.L. 93-579), December 1974.
6. Freedom of Information Act (FOIA), 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048, *Electronic Freedom of Information Act Amendments of 1996.*
7. Health Insurance Portability and Accountability Act (P.L. 104-191), August 1996.
8. The Atomic Energy Act of 1954 (P.L. 83-703), August 1954.

POLICIES, DIRECTIVES, REGULATIONS, AND MEMORANDA

1. Code of Federal Regulations, Title 5, *Administrative Personnel*, Section 731.106, *Designation of Public Trust Positions and Investigative Requirements* (5 C.F.R. 731.106).
2. Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305).
3. Director of Central Intelligence Directive 6/9, *Physical Security Standards For Sensitive Compartmented Information Facilities*, November 2002.
4. Federal Continuity Directive 1 (FCD 1), *Federal Executive Branch National Continuity Program and Requirements*, February 2008.
5. Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 2003.
6. Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004.
7. Intelligence Community Directive Number 704, *Personnel Security Standards and Procedures Governing Eligibility For Access To Sensitive Compartmented Information And Other Controlled Access Program Information*, October 2008.
8. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
9. Office of Management and Budget, Federal Enterprise Architecture Program Management Office, *FEA Consolidated Reference Model Document*, Version 2.3, October 2007.
10. Office of Management and Budget, *Federal Segment Architecture Methodology (FSAM)*, January 2009.

11. Office of Management and Budget Memorandum M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, December 2000.

12. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

13. Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 2003.

14. Office of Management and Budget Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 2003.

15. Office of Management and Budget Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003.

16. Office of Management and Budget Memorandum M-04-26, *Personal Use Policies and File Sharing Technology*, September 2004.

17. Office of Management and Budget Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*, February 2005.

18. Office of Management and Budget Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2005.

19. Office of Management and Budget Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 2006.

20. Office of Management and Budget Memorandum M-06-16, *Protection of Sensitive Information*, June 2006.

21. Office of Management and Budget Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006.

22. Office of Management and Budget Memorandum, *Recommendations for Identity Theft Related Data Breach Notification Guidance*, September 2006.

23. Office of Management and Budget Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 2007.

24. Office of Management and Budget Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007.

25. Office of Management and Budget Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, June 2007.

26. Office of Management and Budget Memorandum M-08-09, *New FISMA Privacy Reporting Requirements for FY 2008*, January 2008.

27. Office of Management and Budget Memorandum M-08-21, *FY08 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, July 2008.

28. Office of Management and Budget Memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration (FDCC)*, August 2008.

29. Office of Management and Budget Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*, August 2008.

30. The White House, Office of the Press Secretary, *Designation and Sharing of Controlled Unclassified Information (CUI)*, May 2008.

31. The White House, Office of the Press Secretary, *Classified Information and Controlled Unclassified Information*, May 2009.

STANDARDS

1. International Organization for Standardization/International Electrotechnical Commission 27001, *Information Security Management System Requirements*, October 2005.

2. International Organization for Standardization/International Electrotechnical Commission 15408-1, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*, October 2005.

3. International Organization for Standardization/International Electrotechnical Commission 15408-2, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements*, October 2005.

4. International Organization for Standardization/International Electrotechnical Commission 15408-3, *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements*, October 2005.

5. National Institute of Standards and Technology Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*, May 2001.

   National Institute of Standards and Technology Federal Information Processing Standards Publication 140-3 (Draft), *Security Requirements for Cryptographic Modules*, July 2007.

6. National Institute of Standards and Technology Federal Information Processing Standards Publication 180-3, *Secure Hash Standard (SHS)*, October 2008.

7. National Institute of Standards and Technology Federal Information Processing Standards Publication 186-3, *Digital Signature Standard (DSS)*, June 2009.

8. National Institute of Standards and Technology Federal Information Processing Standards Publication 188, *Standard Security Labels for Information Transfer*, September 1994.

9. National Institute of Standards and Technology Federal Information Processing Standards Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 1994.

10. National Institute of Standards and Technology Federal Information Processing Standards Publication 197, *Advanced Encryption Standard (AES)*, November 2001.

11. National Institute of Standards and Technology Federal Information Processing Standards Publication 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*, July 2008.

12. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

13. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
14. National Institute of Standards and Technology Federal Information Processing Standards Publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006.
15. Committee for National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.
16. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 7003, *Protective Distribution Systems (PDS)*, December 1996.

GUIDELINES

1. National Institute of Standards and Technology Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, October 1995.
2. National Institute of Standards and Technology Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network*, October 1995.
3. National Institute of Standards and Technology Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September 1996.
4. National Institute of Standards and Technology Special Publication 800-15, *Minimum Interoperability Specification for PKI Components (MISPC),* Version 1, September 1997.
5. National Institute of Standards and Technology Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.
6. National Institute of Standards and Technology Special Publication 800-17, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, February 1998.
7. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
8. National Institute of Standards and Technology Special Publication 800-19, *Mobile Agent Security*, October 1999.
9. National Institute of Standards and Technology Special Publication 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS)*: *Requirements and Procedures*, April 2000.
10. National Institute of Standards and Technology Special Publication 800-21-1, *Second Edition, Guideline for Implementing Cryptography in the Federal Government*, December 2005.
11. National Institute of Standards and Technology Special Publication 800-22, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*, May 2001.
12. National Institute of Standards and Technology Special Publication 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, August 2000.

13. National Institute of Standards and Technology Special Publication 800-24, *PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*, August 2000.

14. National Institute of Standards and Technology Special Publication 800-25, *Federal Agency Use of Public Key Technology for Digital Signatures and Authentication*, October 2000.

15. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.

16. National Institute of Standards and Technology Special Publication 800-28, Version 2, *Guidelines on Active Content and Mobile Code*, March 2008.

17. National Institute of Standards and Technology Special Publication 800-29, *A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2*, June 2001.

18. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

19. National Institute of Standards and Technology Special Publication 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*, February 2001.

20. National Institute of Standards and Technology Special Publication 800-33, *Underlying Technical Models for Information Technology Security*, December 2001.

21. National Institute of Standards and Technology Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

22. National Institute of Standards and Technology Special Publication 800-35, *Guide to Information Technology Security Services*, October 2003.

23. National Institute of Standards and Technology Special Publication 800-36, *Guide to Selecting Information Security Products*, October 2003.

24. National Institute of Standards and Technology Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

25. National Institute of Standards and Technology Special Publication 800-38A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*, December 2001.

26. National Institute of Standards and Technology Special Publication 800-38B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, May 2005.

27. National Institute of Standards and Technology Special Publication 800-38C, *Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality*, May 2004.

28. National Institute of Standards and Technology Special Publication 800-38D, *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) for Confidentiality and Authentication*, November 2007.

29. National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

30. National Institute of Standards and Technology Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*, November 2005.

31. National Institute of Standards and Technology Special Publication 800-41, Revision 1 (Draft), *Guidelines on Firewalls and Firewall Policy*, July 2008.

32. National Institute of Standards and Technology Special Publication 800-43, *Systems Administration Guidance for Windows 2000 Professional*, November 2002.

33. National Institute of Standards and Technology Special Publication 800-44, Version 2, *Guidelines on Securing Public Web Servers*, September 2007.

34. National Institute of Standards and Technology Special Publication 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007.

35. National Institute of Standards and Technology Special Publication 800-46, Revision 1, *Guide to Enterprise Telework and Remote Access Security*, June 2009.

36. National Institute of Standards and Technology Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002.

37. National Institute of Standards and Technology Special Publication 800-48, Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*, July 2008.

38. National Institute of Standards and Technology Special Publication 800-49, *Federal S/MIME V3 Client Profile*, November 2002.

39. National Institute of Standards and Technology Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

40. National Institute of Standards and Technology Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

41. National Institute of Standards and Technology Special Publication 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, June 2005.

42. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008.

43. National Institute of Standards and Technology Special Publication 800-54, *Border Gateway Protocol Security*, July 2007.

44. National Institute of Standards and Technology Special Publication 800-55, Revision 1, *Performance Measurement Guide for Information Security*, July 2008.

45. National Institute of Standards and Technology Special Publication 800-56A (Revised), *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007.

46. National Institute of Standards and Technology Special Publication 800-57 (Revised), *Recommendation for Key Management*, March 2007.

47. National Institute of Standards and Technology Special Publication 800-58, *Security Considerations for Voice Over IP Systems*, January 2005.

48. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

49. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

50. National Institute of Standards and Technology Special Publication 800-61, Revision 1, *Computer Security Incident Handling Guide*, March 2008.

51. National Institute of Standards and Technology Special Publication 800-63-1 (Draft), *Electronic Authentication Guideline*, December 2008.

52. National Institute of Standards and Technology Special Publication 800-64, Revision 2, *Security Considerations in the System Development Life Cycle*, October 2008.

53. National Institute of Standards and Technology Special Publication 800-65, *Integrating Security into the Capital Planning and Investment Control Process*, January 2005.

54. National Institute of Standards and Technology Special Publication 800-66, Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, October 2008.

55. National Institute of Standards and Technology Special Publication 800-67, Version 1.1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2008.

56. National Institute of Standards and Technology Special Publication 800-68, Revision 1, *Guide to Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2008.

57. National Institute of Standards and Technology Special Publication 800-69, *Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist*, September 2006.

58. National Institute of Standards and Technology Special Publication 800-70, Revision 1 (Draft), *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2008.

59. National Institute of Standards and Technology Special Publication 800-72, *Guidelines on PDA Forensics*, November 2004.

60. National Institute of Standards and Technology Special Publication 800-73-2, *Interfaces for Personal Identity Verification*, September 2008.

61. National Institute of Standards and Technology Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, January 2007.

62. National Institute of Standards and Technology Special Publication 800-77, *Guide to IPsec VPNs*, December 2005.

63. National Institute of Standards and Technology Special Publication 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, August 2007.

64. National Institute of Standards and Technology Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, June 2008.

65. National Institute of Standards and Technology Special Publication 800-81, *Secure Domain Name System (DNS) Deployment Guide*, May 2006.

66. National Institute of Standards and Technology Special Publication 800-82 (Final Public Draft), *Guide to Industrial Control Systems (ICS) Security*, September 2008.

67. National Institute of Standards and Technology Special Publication 800-83, *Guide to Malware Incident Prevention and Handling*, November 2005.

68. National Institute of Standards and Technology Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

69. National Institute of Standards and Technology Special Publication 800-85A-1, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)*, March 2009.

70. National Institute of Standards and Technology Special Publication 800-85B, *PIV Data Model Test Guidelines*, July 2006.

71. National Institute of Standards and Technology Special Publication 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

72. National Institute of Standards and Technology Special Publication 800-87, Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, April 2008.

73. National Institute of Standards and Technology Special Publication 800-88, *Guidelines for Media Sanitization*, September 2006.

74. National Institute of Standards and Technology Special Publication 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*, November 2006.

75. National Institute of Standards and Technology Special Publication 800-90 (Revised), *Recommendation for Random Number Generation Using Deterministic Random Bit Generators,* March 2007.

76. National Institute of Standards and Technology Special Publication 800-92, *Guide to Computer Security Log Management*, September 2006.

77. National Institute of Standards and Technology Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*, February 2007.

78. National Institute of Standards and Technology Special Publication 800-95, *Guide to Secure Web Services*, August 2007.

79. National Institute of Standards and Technology Special Publication 800-96, *PIV Card / Reader Interoperability Guidelines*, September 2006.

80. National Institute of Standards and Technology Special Publication 800-97, *Establishing Robust Security Networks: A Guide to IEEE 802.11i*, February 2007.

81. National Institute of Standards and Technology Special Publication 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems,* April 2007.

82. National Institute of Standards and Technology Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.

83. National Institute of Standards and Technology Special Publication 800-101, *Guidelines on Cell Phone Forensics*, May 2007.

84. National Institute of Standards and Technology Special Publication 800-103 (Draft), *An Ontology of Identity Credentials, Part I: Background and Formulation*, October 2006.

85. National Institute of Standards and Technology Special Publication 800-104, *A Scheme for PIV Visual Card Topography*, June 2007.

86. National Institute of Standards and Technology Special Publication 800-106, *Randomized Hashing Digital Signatures*, February 2009.

87. National Institute of Standards and Technology Special Publication 800-107, *Recommendation for Using Approved Hash Algorithms*, February 2009.

88. National Institute of Standards and Technology Special Publication 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*, November 2008.

89. National Institute of Standards and Technology Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007.

90. National Institute of Standards and Technology Special Publication 800-113, *Guide to SSL VPNs*, July 2008.

91. National Institute of Standards and Technology Special Publication 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*, November 2007.

92. National Institute of Standards and Technology Special Publication 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008.

93. National Institute of Standards and Technology Special Publication 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)*, November 2008.

94. National Institute of Standards and Technology Special Publication 800-117 (Draft), *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, May 2009.

95. National Institute of Standards and Technology Special Publication 800-118 (Draft), *Guide to Enterprise Password Management*, April 2009.

96. National Institute of Standards and Technology Special Publication 800-121, *Guide to Bluetooth Security*, September 2008.

97. National Institute of Standards and Technology Special Publication 800-122 (Draft), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, January 2009.

98. National Institute of Standards and Technology Special Publication 800-123, *Guide to General Server Security*, July 2008.

99. National Institute of Standards and Technology Special Publication 800-124, *Guidelines on Cell Phone and PDA Security*, October 2008.

100. National Institute of Standards and Technology Special Publication 800-128 (Draft), *Guide for Security Configuration Management of Information Systems*, August 2009.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Adequate Security
[OMB Circular A-130, Appendix III]

Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Agency

See *Executive Agency*.

Attribute-Based Access Control

Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

Authentication
[FIPS 200]

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authenticator

The means used to confirm the identity of a user, processor, or device (e.g., user password or token).

Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See *Authentication*.

Authorization
(to operate)

The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

Authorization Boundary

All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Authorize Processing

See *Authorization*.

Authorizing Official

A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Availability
[44 U.S.C., Sec. 3542]

Ensuring timely and reliable access to and use of information.

Boundary Protection

Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device

A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.

Chief Information Officer
[PL 104-106, Sec. 5125(b)]

Agency official responsible for:

(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;

(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and

(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency.

Note: Organizations subordinate to federal agencies may use the term *Chief Information Officer* to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.

Chief Information Security Officer

See *Senior Agency Information Security Officer*.

Classified Information

Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD).

Commodity Service

An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.

Common Carrier

In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.

Common Control

A security control that is inherited by one or more organizational information systems. See *Security Control Inheritance*.

Compensating Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.

Confidentiality
[44 U.S.C., Sec. 3542]

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control
[CNSSI 4009]

Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.

Controlled Area

Any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Controlled Unclassified Information

A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces *Sensitive But Unclassified (SBU)*.

Countermeasures
[CNSSI 4009]

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.

Defense-in-depth

Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Domain
[CNSSI 4009]

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See *Security Domain*.

Executive Agency
[41 U.S.C., Sec. 403]

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.

External Information System (or Component)

An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Information System Service

An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.

External Information System Service Provider

A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.

External Network

A network not controlled by the organization.

Failover

The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination of the previously active system.

Federal Agency

See *Executive Agency*.

Federal Enterprise Architecture
[FEA Program Management Office]

A business-based framework for governmentwide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System
[40 U.S.C., Sec. 11331]

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

FIPS-Validated Cryptography

A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See *NSA-Approved Cryptography*.

Guard (System)
[CNSSI 4009, Adapted]

A mechanism limiting the exchange of information between information systems or subsystems.

High-Impact System
[FIPS 200]

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.

Hybrid Security Control

A security control that is implemented in an information system in part as a common control and in part as a system-specific control.

See *Common Control* and *System-Specific Security Control*.

Identity-Based Access Control

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

Incident
[FIPS 200]

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Industrial Control System

An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.

Information
[FIPS 199]

An instance of an information type.

Information Owner
[CNSSI 4009]

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Resources
[44 U.S.C., Sec. 3502]

Information and related resources, such as personnel, equipment, funds, and information technology.

Information Security
[44 U.S.C., Sec. 3542]

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information Security Policy
[CNSSI 4009]

Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

Information Security Program Plan

Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Information System
[44 U.S.C., Sec. 3502]

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.]

Information System Owner
(or Program Manager)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

Information System
Security Officer
[CNSSI 4009]

Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

Information Technology
[40 U.S.C., Sec. 1401]

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Information Type
[FIPS 199]

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Integrity
[44 U.S.C., Sec. 3542]

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Internal Network

A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.

Label

See *Security Label*.

Line of Business

The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.

Local Access

Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.

Low-Impact System
[FIPS 200]

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.

Malicious Code

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware

See *Malicious Code*.

Management Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.

Marking

See *Security Marking*.

Media
[FIPS 200]

Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

Mobile Code

Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Mobile Code Technologies

Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).

Mobile Device

Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory).

Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

Moderate-Impact System
[FIPS 200]

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high.

Multifactor Authentication

Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See *Authenticator*.

National Security Emergency Preparedness Telecommunications Services
[47 C.F.R., Part 64, App A]

Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.

National Security System
[44 U.S.C., Sec. 3542]

Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Network
[CNSSI 4009]

Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

Network Access

Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Non-Local Maintenance

Maintenance activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network.

Non-Organizational User

A user who is not an organizational user (including public users).

Non-repudiation

Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

NSA-Approved Cryptography

Cryptography that consists of: (i) an approved algorithm; (ii) an implementation that has been approved for the protection of classified information in a particular environment; and (iii) a supporting key management infrastructure.

Object

Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See *Subject*.

Operational Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).

Organization
[FIPS 200, Adapted]

An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

Organizational User

An organizational employee or an individual the organization deems to have equivalent status of an employee (e.g., contractor, guest researcher, individual detailed from another organization, individual from allied nation).

Penetration Testing

A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

Plan of Action and Milestones
[OMB Memorandum 02-01]

A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Potential Impact
[FIPS 199]

The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.

Privacy Impact Assessment
[OMB Memorandum 03-22]

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privileged Account

An information system account with authorizations of a privileged user.

Privileged Command

A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.

Privileged User
[CNSSI 4009]

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Protective Distribution System

Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.

Reciprocity

Mutual agreement among participating enterprises to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

Records

The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).

Red Team Exercise

An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.

Remote Access

Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Remote Maintenance

Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).

Removable Media

Portable electronic storage media such as magnetic, optical, and solid state devices, which can be inserted into and removed from a computing device, and that is used to store text, video, audio, and image information. Examples include hard disks, floppy disks, zip drives, compact disks, thumb drives, pen drives, and similar USB storage devices.

Restricted Data
[Atomic Energy Act of 1954]

All data concerning (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 [of the Atomic Energy Act of 1954].

Risk
[FIPS 200, Adapted]

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Assessment

The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.

Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management
[FIPS 200, Adapted]

The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

Role-Based Access Control

Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

Safeguards
[CNSSI 4009]

Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Sanitization

A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.

Scoping Guidance

A part of tailoring guidance providing organizations with specific policy/regulatory-related, technology-related, system component allocation-related, operational/environmental-related, physical infrastructure-related, public access-related, scalability-related, common control-related, and security objective-related considerations on the applicability and implementation of individual security controls in the security control baseline.

Security Attribute

An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.

Security Authorization

See *Authorization*.

Security Authorization Boundary

See *Authorization Boundary*.

Security Categorization

The process of determining the security category for information or an information system. See *Security Category*.

Security Category
[FIPS 199, Adapted]

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Security Control Assessment

The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security Control Baseline
[FIPS 200]

The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system.

Security Control Enhancements

Statements of security capability to: (i) build in additional, but related, functionality to a security control; and/or (ii) increase the strength of the control.

Security Control Inheritance

A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.

Security Controls
[FIPS 199]

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Domain
[CNSSI 4009]

A domain that implements a security policy and is administered by a single authority.

Security Functions

The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.

Security Impact Analysis

The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

Security Incident

See *Incident*.

Security Label

The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.

Security Marking

Human-readable information affixed to information system components, removable media, or output indicating the distribution limitations, handling caveats and applicable security markings.

Security Objective
[FIPS 199]

Confidentiality, integrity, or availability.

Security Plan

Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

See *System Security Plan* or *Information Security Program Plan*.

Security Policy
[CNSSI 4009]

A set of criteria for the provision of security services.

Security Requirements
[FIPS 200]

Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Security-Relevant Information

Any information within the information system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.

Senior (Agency) Information Security Officer
[44 U.S.C., Sec. 3544]

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.

Senior Information Security Officer

See *Senior Agency Information Security Officer*.

Sensitive Information
[CNSSI 4009]

Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Sensitive Compartmented Information
[CNSSI 4009]

Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Special Access Program
[CNSSI 4009]

A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.

Spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Subject

Generally an individual, process, or device causing information to flow among objects or change to the system state. See *Object*.

Subsystem

A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.

Supply Chain

A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

System

See *Information System*.

System Security Plan
[NIST SP 800-18]

Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

System-Specific Security Control

A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

Tailored Security Control Baseline

A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.

Tailoring

The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

Technical Controls
[FIPS 200]

The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat
[CNSSI 4009, Adapted]

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Threat Assessment
[CNSSI 4009]

Formal description and evaluation of threat to an information system.

Threat Source
[FIPS 200]

The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.

Trusted Path

A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.

User
[CNSSI 4009, adapted]

Individual, or (system) process acting on behalf of an individual, authorized to access an information system.

See *Organizational User* and *Non-Organizational User*.

Vulnerability
[CNSSI 4009]

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment
[CNSSI 4009]

Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
DNS	Domain Name System
DOD	Department of Defense
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information System Security Instruction
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RD	Restricted Data
SAISO	Senior Agency Information Security Officer
SAMI	Sources And Methods Information
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
TSP	Telecommunications Service Priority
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

APPENDIX D

SECURITY CONTROL BASELINES – SUMMARY

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

This appendix contains the security control baselines that represent the starting point in determining the security controls for low-impact, moderate-impact, and high-impact information systems.[71] The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines.[72] If a security control is selected for one of the baselines, the security control family identifier and control number are listed in the appropriate column. If a control is not used in a particular baseline, the entry is marked "not selected." Control enhancements, when used to supplement security controls, are indicated by the number of the control enhancement. For example, an "IR-2 (1)" in the high baseline entry for the IR-2 security control indicates that the second control from the Incident Response family has been selected along with control enhancement (1). Note that some security controls and enhancements in the security control catalog are not used in any of the baselines in this appendix but are available for use by organizations if needed; for example, when the results of a risk assessment indicate the need for additional controls or control enhancements in order to adequately mitigate risk to organizational operations and organizational assets, individuals, other organizations, and the Nation.

Organizations can use the recommended *priority code* designation associated with each security control in the baselines to assist in making sequencing decisions for control implementation (i.e., a Priority Code 1 [P1] control has a higher priority for implementation than a Priority Code 2 [P2] control; a Priority Code 2 (P2) control has a higher priority for implementation than a Priority Code 3 [P3] control). This recommended sequencing prioritization helps ensure that foundational security controls upon which other controls depend are implemented first, thus enabling organizations to deploy controls in a more structured and timely manner in accordance with available resources. The implementation of security controls by sequence priority code does not imply the achievement of any defined level of risk mitigation until *all* of the security controls in the security plan have been implemented. The priority codes are used only for implementation sequencing, not for making security control selection decisions. Table D-1 summarizes sequence priority codes for the baseline security controls in Table D-2.

TABLE D-1: SECURITY CONTROL PRIORITIZATION CODES

Priority Code	Sequencing	Action
Priority Code 1 (P1)	FIRST	Implement P1 security controls first.
Priority Code 2 (P2)	NEXT	Implement P2 security controls after implementation of P1 controls.
Priority Code 3 (P3)	LAST	Implement P3 security controls after implementation of P1 and P2 controls.
Unspecified Priority Code (P0)	NONE	Security control not selected for baseline.

[71] A complete description of all security controls is provided in Appendices F and G. In addition, separate documents for individual security control baselines (listed as Annexes 1, 2, and 3) are available at http://csrc.nist.gov/publications.

[72] The hierarchical nature applies to the security requirements of each control (i.e., the base control plus all of its enhancements) at the low-impact, moderate-impact, and high-impact level in that the control requirements at a particular impact level (e.g., CP-4 *Contingency Plan Testing and Exercises*—Moderate: CP-4 (1)) meets a stronger set of security requirements for that control than the next lower impact level of the same control (e.g., CP-4 *Contingency Plan Testing and Exercises*—Low: CP-4).

In addition to Table D-2, the sequence priority codes and security control baselines are annotated in a priority and baseline allocation summary section below each security control in Appendix F.

TABLE D-2: SECURITY CONTROL BASELINES

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
Access Control					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2)	AC-6 (1) (2)
AC-7	Unsuccessful Login Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P2	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11	AC-11
AC-12	Session Termination (Withdrawn)	---	---	---	---
AC-13	Supervision and Review—Access Control (Withdrawn)	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P1	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking (Withdrawn)	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2) (3) (4) (5) (7) (8)	AC-17 (1) (2) (3) (4) (5) (7) (8)
AC-18	Wireless Access	P1	AC-18	AC-18 (1)	AC-18 (1) (2) (4) (5)
AC-19	Access Control for Mobile Devices	P1	AC-19	AC-19 (1) (2) (3)	AC-19 (1) (2) (3)
AC-20	Use of External Information Systems	P1	AC-20	AC-20 (1) (2)	AC-20 (1) (2)
AC-21	User-Based Collaboration and Information Sharing	P0	Not Selected	Not Selected	Not Selected
AC-22	Publicly Accessible Content	P2	AC-22	AC-22	AC-22
Awareness and Training					
AT-1	Security Awareness and Training Policy and Procedures	P1	AT-1	AT-1	AT-1
AT-2	Security Awareness	P1	AT-2	AT-2	AT-2
AT-3	Security Training	P1	AT-3	AT-3	AT-3
AT-4	Security Training Records	P3	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	P0	Not Selected	Not Selected	Not Selected
Audit and Accountability					
AU-1	Audit and Accountability Policy and Procedures	P1	AU-1	AU-1	AU-1
AU-2	Auditable Events	P1	AU-2	AU-2 (3) (4)	AU-2 (3) (4)

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
AU-3	Content of Audit Records	P1	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	P1	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	P1	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Review, Analysis, and Reporting	P1	AU-6	AU-6	AU-6 (1)
AU-7	Audit Reduction and Report Generation	P2	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	P1	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	P1	AU-9	AU-9	AU-9
AU-10	Non-repudiation	P1	Not Selected	Not Selected	AU-10
AU-11	Audit Record Retention	P3	AU-11	AU-11	AU-11
AU-12	Audit Generation	P1	AU-12	AU-12	AU-12 (1)
AU-13	Monitoring for Information Disclosure	P0	Not Selected	Not Selected	Not Selected
AU-14	Session Audit	P0	Not Selected	Not Selected	Not Selected
Security Assessment and Authorization					
CA-1	Security Assessment and Authorization Policies and Procedures	P1	CA-1	CA-1	CA-1
CA-2	Security Assessments	P2	CA-2	CA-2 (1)	CA-2 (1) (2)
CA-3	Information System Connections	P1	CA-3	CA-3	CA-3
CA-4	Security Certification (Withdrawn)	---	---	---	---
CA-5	Plan of Action and Milestones	P3	CA-5	CA-5	CA-5
CA-6	Security Authorization	P3	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	P3	CA-7	CA-7	CA-7
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (4)	CM-2 (1) (2) (3) (5) (6)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	P1	CM-6	CM-6 (3)	CM-6 (1) (2) (3)
CM-7	Least Functionality	P1	CM-7	CM-7 (1)	CM-7 (1) (2)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
Contingency Planning					
CP-1	Contingency Planning Policy and Procedures	P1	CP-1	CP-1	CP-1
CP-2	Contingency Plan	P1	CP-2	CP-2 (1)	CP-2 (1) (2) (3)
CP-3	Contingency Training	P2	CP-3	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	P2	CP-4	CP-4 (1)	CP-4 (1) (2) (4)
CP-5	Contingency Plan Update (Withdrawn)	---	---	---	---
CP-6	Alternate Storage Site	P1	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	P1	Not Selected	CP-7 (1) (2) (3) (5)	CP-7 (1) (2) (3) (4) (5)

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
CP-8	Telecommunications Services	P1	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	P1	CP-9	CP-9 (1)	CP-9 (1) (2) (3)
CP-10	Information System Recovery and Reconstitution	P1	CP-10	CP-10 (2) (3)	CP-10 (2) (3) (4)
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1)	IA-2 (1) (2) (3) (8)	IA-2 (1) (2) (3) (4) (8) (9)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1)	IA-5 (1) (2) (3)	IA-5 (1) (2) (3)
IA-6	Authenticator Feedback	P1	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8	IA-8	IA-8
Incident Response					
IR-1	Incident Response Policy and Procedures	P1	IR-1	IR-1	IR-1
IR-2	Incident Response Training	P2	IR-2	IR-2	IR-2 (1) (2)
IR-3	Incident Response Testing and Exercises	P2	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	P1	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	P1	IR-5	IR-5	IR-5 (1)
IR-6	Incident Reporting	P1	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	P3	IR-7	IR-7 (1)	IR-7 (1)
IR-8	Incident Response Plan	P1	IR-8	IR-8	IR-8
Maintenance					
MA-1	System Maintenance Policy and Procedures	P1	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	P2	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	P2	Not Selected	MA-3 (1) (2)	MA-3 (1) (2) (3)
MA-4	Non-Local Maintenance	P1	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	P1	MA-5	MA-5	MA-5
MA-6	Timely Maintenance	P1	Not Selected	MA-6	MA-6
Media Protection					
MP-1	Media Protection Policy and Procedures	P1	MP-1	MP-1	MP-1
MP-2	Media Access	P1	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Marking	P1	Not Selected	MP-3	MP-3
MP-4	Media Storage	P1	Not Selected	MP-4	MP-4
MP-5	Media Transport	P1	Not Selected	MP-5 (2) (4)	MP-5 (2) (3) (4)
MP-6	Media Sanitization	P1	MP-6	MP-6	MP-6 (1) (2) (3)
Physical and Environmental Protection					
PE-1	Physical and Environmental Protection Policy and Procedures	P1	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	P1	PE-2	PE-2	PE-2
PE-3	Physical Access Control	P1	PE-3	PE-3	PE-3 (1)

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
PE-4	Access Control for Transmission Medium	P1	Not Selected	PE-4	PE-4
PE-5	Access Control for Output Devices	P1	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	P1	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	P1	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	P3	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	P1	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	P1	Not Selected	PE-10	PE-10
PE-11	Emergency Power	P1	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	P1	PE-12	PE-12	PE-12
PE-13	Fire Protection	P1	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	P1	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	P1	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	P1	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	P1	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	P2	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	P0	Not Selected	Not Selected	Not Selected
Planning					
PL-1	Security Planning Policy and Procedures	P1	PL-1	PL-1	PL-1
PL-2	System Security Plan	P1	PL-2	PL-2	PL-2
PL-3	System Security Plan Update (Withdrawn)	---	---	---	---
PL-4	Rules of Behavior	P1	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	P1	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	P3	Not Selected	PL-6	PL-6
Personnel Security					
PS-1	Personnel Security Policy and Procedures	P1	PS-1	PS-1	PS-1
PS-2	Position Categorization	P1	PS-2	PS-2	PS-2
PS-3	Personnel Screening	P1	PS-3	PS-3	PS-3
PS-4	Personnel Termination	P2	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	P2	PS-5	PS-5	PS-5
PS-6	Access Agreements	P3	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	P1	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	P3	PS-8	PS-8	PS-8
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update (Withdrawn)	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1)	RA-5 (1) (2) (3) (4) (5) (7)
System and Services Acquisition					
SA-1	System and Services Acquisition Policy and Procedures	P1	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	P1	SA-2	SA-2	SA-2

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
SA-3	Life Cycle Support	P1	SA-3	SA-3	SA-3
SA-4	Acquisitions	P1	SA-4	SA-4 (1) (4)	SA-4 (1) (2) (4)
SA-5	Information System Documentation	P2	SA-5	SA-5 (1) (3)	SA-5 (1) (2) (3)
SA-6	Software Usage Restrictions	P1	SA-6	SA-6	SA-6
SA-7	User-Installed Software	P1	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	P1	Not Selected	SA-8	SA-8
SA-9	External Information System Services	P1	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	P1	Not Selected	SA-10	SA-10
SA-11	Developer Security Testing	P2	Not Selected	SA-11	SA-11
SA-12	Supply Chain Protection	P1	Not Selected	Not Selected	SA-12
SA-13	Trustworthiness	P1	Not Selected	Not Selected	SA-13
SA-14	Critical Information System Components	P0	Not Selected	Not Selected	Not Selected
System and Communications Protection					
SC-1	System and Communications Protection Policy and Procedures	P1	SC-1	SC-1	SC-1
SC-2	Application Partitioning	P1	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	P1	Not Selected	Not Selected	SC-3
SC-4	Information in Shared Resources	P1	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	P1	SC-5	SC-5	SC-5
SC-6	Resource Priority	P0	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	P1	SC-7	SC-7 (1) (2) (3) (4) (5) (7)	SC-7 (1) (2) (3) (4) (5) (6) (7) (8)
SC-8	Transmission Integrity	P1	Not Selected	SC-8 (1)	SC-8 (1)
SC-9	Transmission Confidentiality	P1	Not Selected	SC-9 (1)	SC-9 (1)
SC-10	Network Disconnect	P2	Not Selected	SC-10	SC-10
SC-11	Trusted Path	P0	Not Selected	Not Selected	Not Selected
SC-12	Cryptographic Key Establishment and Management	P1	SC-12	SC-12	SC-12 (1)
SC-13	Use of Cryptography	P1	SC-13	SC-13	SC-13
SC-14	Public Access Protections	P1	SC-14	SC-14	SC-14
SC-15	Collaborative Computing Devices	P1	SC-15	SC-15	SC-15
SC-16	Transmission of Security Attributes	P0	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	P1	Not Selected	SC-17	SC-17
SC-18	Mobile Code	P1	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	P1	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	P1	SC-20 (1)	SC-20 (1)	SC-20 (1)
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	P1	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	P1	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	P1	Not Selected	SC-23	SC-23
SC-24	Fail in Known State	P1	Not Selected	Not Selected	SC-24
SC-25	Thin Nodes	P0	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	PRIORITY	CONTROL BASELINES		
			LOW	MOD	HIGH
SC-26	Honeypots	P0	Not Selected	Not Selected	Not Selected
SC-27	Operating System-Independent Applications	P0	Not Selected	Not Selected	Not Selected
SC-28	Protection of Information at Rest	P1	Not Selected	SC-28	SC-28
SC-29	Heterogeneity	P0	Not Selected	Not Selected	Not Selected
SC-30	Virtualization Techniques	P0	Not Selected	Not Selected	Not Selected
SC-31	Covert Channel Analysis	P0	Not Selected	Not Selected	Not Selected
SC-32	Information System Partitioning	P0	Not Selected	SC-32	SC-32
SC-33	Transmission Preparation Integrity	P0	Not Selected	Not Selected	Not Selected
SC-34	Non-Modifiable Executable Programs	P0	Not Selected	Not Selected	Not Selected
System and Information Integrity					
SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2) (3)	SI-3 (1) (2) (3)
SI-4	Information System Monitoring	P1	Not Selected	SI-4 (2) (4) (5) (6)	SI-4 (2) (4) (5) (6)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	P1	Not Selected	SI-7 (1)	SI-7 (1) (2)
SI-8	Spam Protection	P1	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	P2	Not Selected	SI-9	SI-9
SI-10	Information Input Validation	P1	Not Selected	SI-10	SI-10
SI-11	Error Handling	P2	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	P2	SI-12	SI-12	SI-12
SI-13	Predictable Failure Prevention	P0	Not Selected	Not Selected	Not Selected
Program Management					
PM-1	Information Security Program Plan	P1	**Deployed organization-wide Supporting all baselines**		
PM-2	Senior Information Security Officer	P1			
PM-3	Information Security Resources	P1			
PM-4	Plan of Action and Milestones Process	P1			
PM-5	Information System Inventory	P1			
PM-6	Information Security Measures of Performance	P1			
PM-7	Enterprise Architecture	P1			
PM-8	Critical Infrastructure Plan	P1			
PM-9	Risk Management Strategy	P1			
PM-10	Security Authorization Process	P1			
PM-11	Mission/Business Process Definition	P1			

APPENDIX E

MINIMUM ASSURANCE REQUIREMENTS

LOW-IMPACT, MODERATE-IMPACT, AND HIGH-IMPACT INFORMATION SYSTEMS

The minimum assurance requirements for security controls described in the security control catalog are listed below. The assurance requirements are directed at the activities and actions that security control developers and implementers[73] define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The assurance requirements are applied on a control-by-control basis. The requirements are grouped by information system impact level (i.e., low, moderate, and high) since the requirements apply to each control within the respective impact level. Using a format similar to security controls, assurance requirements are followed by supplemental guidance that provides additional detail and explanation of how the requirements are to be applied. Bolded text indicates requirements that appear for the first time at a particular impact level.

Low-Impact Information Systems

Assurance Requirement: **The security control is in effect and meets explicitly identified functional requirements in the control statement.**

Supplemental Guidance: For security controls in low-impact information systems, the focus is on the controls being in place with the expectation that no obvious errors exist and that, as flaws are discovered, they are addressed in a timely manner.

Moderate-Impact Information Systems

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. **The control developer/implementer provides a description of the functional properties of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will meet its required function or purpose. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.**

Supplemental Guidance: For security controls in moderate-impact information systems, the focus is on actions supporting increased confidence in the correct implementation and operation of the control. While flaws are still likely to be uncovered (and addressed expeditiously), the control developer/implementer incorporates, as part of the control, specific capabilities and produces specific documentation supporting increased confidence that the control meets its required function or purpose. This documentation is also needed by assessors to analyze and test the functional properties of the control as part of the overall assessment of the control.

Note: This level of assurance is not intended to protect a moderate-impact information system against high-end threat agents (i.e., threat agents that are highly skilled, highly motivated, and well-resourced). When such protection is required, the section below entitled *Additional Assurance Requirements for Moderate-Impact and High-Impact Information Systems* applies.

[73] In this context, a developer/implementer is an individual or group of individuals responsible for the development or implementation of security controls. This may include in addition to organizational personnel, for example, hardware and software vendors providing the controls and contractors implementing the controls.

High-Impact Information Systems

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties **and design/implementation** of the control with sufficient detail to permit analysis and testing of the control (**including functional interfaces among control components)**. The control developer/implementer includes as an integral part of the control, assigned responsibilities and specific actions supporting increased confidence that when the control is implemented, it will **continuously and consistently (i.e., across the information system)** meet its required function or purpose **and support improvement in the effectiveness of the control**. These actions include, for example, requiring the development of records with structure and content suitable to facilitate making this determination.

Supplemental Guidance: For security controls in high-impact information systems, the focus is expanded to require, within the control, the capabilities that are needed to support ongoing consistent operation of the control and continuous improvement in the control's effectiveness. The developer/implementer is expected to expend significant effort on the design, development, implementation, and component/integration testing of the controls and to produce associated design and implementation documentation to support these activities. This documentation is also needed by assessors to analyze and test the internal components of the control as part of the overall assessment of the control.

Note: This level of assurance is not intended to protect a high-impact information system against high-end threat agents (i.e., threat agents that are highly skilled, highly motivated, and well-resourced). When such protection is required, the section below entitled *Additional Assurance Requirements for Moderate-Impact and High-Impact Information Systems* applies.

Additional Assurance Requirements for Moderate-Impact and High-Impact Information Systems

Assurance Requirement: The security control is in effect and meets explicitly identified functional requirements in the control statement. The control developer/implementer provides a description of the functional properties and design/implementation of the control with sufficient detail to permit analysis and testing of the control. The control developer/implementer includes as an integral part of the control, actions supporting increased confidence that when the control is implemented, it will continuously and consistently (i.e., across the information system) meet its required function or purpose and support improvement in the effectiveness of the control. These actions include requiring the development of records with structure and content suitable to facilitate making this determination. **The control is developed in a manner that supports a high degree of confidence that the control is complete, consistent, and correct.**

Supplemental Guidance: The additional high assurance requirements are intended to supplement the minimum assurance requirements for moderate-impact and high-impact information systems, when appropriate, in order to protect against threats from highly skilled, highly motivated, and well-resourced threat agents. This level of protection is necessary for those information systems where the organization is not willing to accept the risks associated with the type of threat agents cited above.

APPENDIX F

SECURITY CONTROL CATALOG

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

The catalog of security controls in this appendix provides a range of safeguards and countermeasures for organizations and information systems. The organization of the security control catalog, the structure of the controls, and the concept of allocating security controls and control enhancements to the initial baselines in Appendix D are described in Chapter Two. The security controls in the catalog are expected to change over time, as controls are withdrawn, revised and added. In order to maintain stability in security plans and automated tools supporting the implementation of NIST Special Publication 800-53, security controls and control enhancements will not be renumbered each time a control or enhancement is withdrawn. Notations of security controls and controls enhancements that have been withdrawn will be maintained in the catalog for historical purposes.

About the Catalog

Security controls and control enhancements in Appendices F and G are generally designed to be policy-neutral and technology/implementation independent. Additional information about security controls and control enhancements can be provided in two ways:

- By establishing specific values in the variable sections of selected security controls (i.e., *assignment* and *selection* statements); and
- By specifying security control implementation detail (e.g., platform dependencies) in the associated security plan for the information system or security program plan for the organization.

Assignment and selection statements provide organizations with the capability to specialize security controls and control enhancements based on organizational security requirements and/or requirements originating in federal laws, Executive Orders, directives, policies, regulations, standards, or guidelines. Security control enhancements are used to strengthen or broaden the fundamental security capability described in the base control and are not used as a substitute for using assignment or selection statements to add greater specificity to the control. The first security control in each family (a.k.a. the *dash one* control) generates the requirement for policy and procedures that are needed for the effective implementation of the other security controls and control enhancements in the family. Therefore, the individual controls/enhancements in the family typically do not call for the development of such policy and procedures.

Security controls and control enhancements are employed in federal information systems in accordance with the risk management guidance provided in NIST Special Publication 800-39 as summarized in Chapter Three of this publication. This guidance includes selecting baseline security controls (see Appendix D) in accordance with the FIPS 199 security category of the information system and the FIPS 200 system impact level, and subsequently tailoring the baseline. The tailored security control baseline represents the minimum controls for low-impact, moderate-impact, and high-impact information systems, respectively. There are additional security controls and control enhancements that appear in the catalog that are not used in any of the baselines. These additional controls and control enhancements are available to organizations and can be used in supplementing the tailored baselines to achieve the needed level of protection in accordance with an organizational assessment of risk. Moreover, security controls and control enhancements contained in higher-level baselines can also be used in lower-level baselines, if deemed appropriate, to provide additional protection measures.

Beginning with NIST Special Publication 800-53, Revision 3, the supplemental guidance sections for security controls and control enhancements contain no requirements or references to FIPS or NIST Special Publications. NIST publications are included in a new *References* section that has been added to the general description and content of the security control specification. In addition, minimum and maximum values (e.g., testing contingency plans *at least annually*) have been removed from the assignment statements in security controls. Organizations should consult specific federal laws, Executive Orders, directives, policies, regulations, standards, or guidelines as the definitive sources for such information. Removal of minimum and maximum values from the security controls does not obviate the need of organizations to comply with requirements in the controlling source publications.

Finally, in support of the Joint Task Force Transformation Initiative to develop a unified information security framework for the federal government, security controls for national security systems are included in the security control catalog. The inclusion of these security controls is not intended to impose security requirements on organizations that operate national security systems; rather, the controls are available to use on a voluntary basis with the approval of appropriate federal officials exercising policy authority over such systems. In addition, the security control priorities and security control baselines listed in Appendix D and in the priority and baseline allocation summary boxes below each security control in Appendix F, apply to nonnational security systems *only* unless otherwise directed by the aforementioned federal officials with national security policy authority.

≈

FAMILY: ACCESS CONTROL **CLASS:** TECHNICAL

AC-1 ACCESS CONTROL POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the access control family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the access control policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AC-1	**MOD** AC-1	**HIGH** AC-1

AC-2 ACCOUNT MANAGEMENT

Control: The organization manages information system accounts, including:

a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);

b. Establishing conditions for group membership;

c. Identifying authorized users of the information system and specifying access privileges;

d. Requiring appropriate approvals for requests to establish accounts;

e. Establishing, activating, modifying, disabling, and removing accounts;

f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;

g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;

h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;

i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and

j. Reviewing accounts [*Assignment: organization-defined frequency*].

Supplemental Guidance: The identification of authorized users of the information system and the specification of access privileges is consistent with the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by organizational officials responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

(1) **The organization employs automated mechanisms to support the management of information system accounts.**

(2) **The information system automatically terminates temporary and emergency accounts after [*Assignment: organization-defined time period for each type of account*].**

(3) **The information system automatically disables inactive accounts after [*Assignment: organization-defined time period*].**

(4) **The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.**

(5) **The organization:**

(a) **Requires that users log out when [*Assignment: organization defined time-period of expected inactivity and/or description of when to log out*];**

(b) **Determines normal time-of-day and duration usage for information system accounts;**

(c) **Monitors for atypical usage of information system accounts; and**

(d) **Reports atypical usage to designated organizational officials.**

(6) **The information system dynamically manages user privileges and associated access authorizations.**

Enhancement Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of user privileges, many service-oriented architecture implementations rely on run time access control decisions facilitated by dynamic privilege management. While user identities remain relatively constant over time, user privileges may change more frequently based on the ongoing mission/business requirements and operational needs of the organization.

(7) **The organization:**

(a) **Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and**

(b) **Tracks and monitors privileged role assignments.**

Enhancement Supplemental Guidance: Privileged roles include, for example, key management, network and system administration, database administration, web administration.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-2	**MOD** AC-2 (1) (2) (3) (4)	**HIGH** AC-2 (1) (2) (3) (4)

AC-3 ACCESS ENFORCEMENT

Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.

Supplemental Guidance: Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by organizations to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system. In addition to enforcing authorized access at the information-system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Consideration is given to the implementation of an audited, explicit override of automated mechanisms in the event of emergencies or other serious events. If encryption of stored information is employed as an access enforcement mechanism, the cryptography used is FIPS 140-2 (as amended) compliant. For classified information, the cryptography used is largely dependent on the classification level of the information and the clearances of the individuals having access to the information. Mechanisms implemented by AC-3 are configured to enforce authorizations determined by other security controls. Related controls: AC-2, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AC-21, AC-22, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.

Control Enhancements:

(1) [Withdrawn: Incorporated into AC-6].

(2) The information system enforces dual authorization, based on organizational policies and procedures for [*Assignment: organization-defined privileged commands*].

Enhancement Supplemental Guidance: Dual authorization mechanisms require two forms of approval to execute. The organization does not employ dual authorization mechanisms when an immediate response is necessary to ensure public and environmental safety.

(3) The information system enforces [*Assignment: organization-defined nondiscretionary access control policies*] over [*Assignment: organization-defined set of users and resources*] where the policy rule set for each policy specifies:

(a) Access control information (i.e., attributes) employed by the policy rule set (e.g., position, nationality, age, project, time of day); and

(b) Required relationships among the access control information to permit access.

Enhancement Supplemental Guidance: Nondiscretionary access control policies that may be implemented by organizations include, for example, Attribute-Based Access Control, Mandatory Access Control, and Originator Controlled Access Control. Nondiscretionary access control policies may be employed by organizations in addition to the employment of discretionary access control policies.

For Mandatory Access Control (MAC): Policy establishes coverage over all subjects and objects under its control to ensure that each user receives only that information to which the user is authorized access based on classification of the information, and on user clearance and formal access authorization. The information system assigns appropriate security attributes (e.g., labels/security domains/types) to subjects and objects, and uses these attributes as the basis for MAC decisions. The Bell-LaPadula security model defines allowed access with regard to an organization-defined set of strictly hierarchical security levels as follows: A subject can read an object only if the security level of the subject dominates the security level of the object and a subject can write to an object only if two conditions are met: the security level of the object dominates the security level of the subject, and the security level of the user's clearance dominates the security level of the object (no read up, no write down).

For Role-Based Access Control (RBAC): Policy establishes coverage over all users and resources to ensure that access rights are grouped by role name, and access to resources is restricted to users who have been authorized to assume the associated role.

(4) The information system enforces a Discretionary Access Control (DAC) policy that:

(a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both;

(b) Limits propagation of access rights; and

(c) Includes or excludes access to the granularity of a single user.

(5) The information system prevents access to [*Assignment: organization-defined security-relevant information*] except during secure, nonoperable system states.

Enhancement Supplemental Guidance: Security-relevant information is any information within the information system that can potentially impact the operation of security functions in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data. Filtering rules for routers and firewalls, cryptographic key management information, key configuration parameters for security services, and access control lists are examples of security-relevant information. Secure, nonoperable system states are states in which the information system is not performing mission/business-related processing (e.g., the system is off-line for maintenance, troubleshooting, boot-up, shutdown).

(6) The organization encrypts or stores off-line in a secure location [*Assignment: organization-defined user and/or system information*].

Enhancement Supplemental Guidance: The use of encryption by the organization reduces the probability of unauthorized disclosure of information and can also detect unauthorized changes to information. Removing information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access via a network. Related control: MP-4.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-3	**MOD** AC-3	**HIGH** AC-3

AC-4 INFORMATION FLOW ENFORCEMENT

Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.

Control Enhancements:

(1) The information system enforces information flow control using explicit security attributes on information, source, and destination objects as a basis for flow control decisions.

Enhancement Supplemental Guidance: Information flow enforcement mechanisms compare security attributes on all information (data content and data structure), source and destination objects, and respond appropriately (e.g., block, quarantine, alert administrator) when the mechanisms encounter information flows not explicitly allowed by the information flow policy. Information flow enforcement using explicit security attributes can be used, for example, to control the release of certain types of information.

(2) The information system enforces information flow control using protected processing domains (e.g., domain type-enforcement) as a basis for flow control decisions.

(3) The information system enforces dynamic information flow control based on policy that allows or disallows information flows based on changing conditions or operational considerations.

(4) The information system prevents encrypted data from bypassing content-checking mechanisms.

(5) The information system enforces [*Assignment: organization-defined limitations on the embedding of data types within other data types*].

(6) The information system enforces information flow control on metadata.

(7) The information system enforces [*Assignment: organization-defined one-way flows*] using hardware mechanisms.

(8) The information system enforces information flow control using [*Assignment: organization-defined security policy filters*] as a basis for flow control decisions.

Enhancement Supplemental Guidance: Organization-defined security policy filters include, for example, dirty word filters, file type checking filters, structured data filters, unstructured data filters, metadata content filters, and hidden content filters. Structured data permits the interpretation of its content by virtue of atomic elements that are understandable by an application and indivisible. Unstructured data refers to masses of (usually) digital information that does not have a data structure or has a data structure that is not easily readable by a machine. Unstructured data consists of two basic categories: (i) bitmap objects that are inherently non language-based (i.e., image, video, or audio files); and (ii) textual objects that are based on a written or printed language (i.e., commercial off-the-shelf word processing documents, spreadsheets, or emails).

(9) The information system enforces the use of human review for [*Assignment: organization-defined security policy filters*] when the system is not capable of making an information flow control decision.

(10) The information system provides the capability for a privileged administrator to enable/disable [*Assignment: organization-defined security policy filters*].

(11) The information system provides the capability for a privileged administrator to configure [*Assignment: organization-defined security policy filters*] to support different security policies.

Enhancement Supplemental Guidance: For example, to reflect changes in the security policy, an administrator can change the list of “dirty words” that the security policy mechanism checks in accordance with the definitions provided by the organization.

(12) The information system, when transferring information between different security domains, identifies information flows by data type specification and usage.

Enhancement Supplemental Guidance: Data type specification and usage include, for example, using file naming to reflect type of data and limiting data transfer based on file type.

(13) The information system, when transferring information between different security domains, decomposes information into policy-relevant subcomponents for submission to policy enforcement mechanisms.

Enhancement Supplemental Guidance: Policy enforcement mechanisms include the filtering and/or sanitization rules that are applied to information prior to transfer to a different security domain. Parsing transfer files facilitates policy decisions on source, destination, certificates, classification, subject, attachments, and other information security-related component differentiators. Policy rules for cross domain transfers include, for example, limitations on embedding components/information types within other components/information types, prohibiting more than two-levels of embedding, and prohibiting the transfer of archived information types.

(14) The information system, when transferring information between different security domains, implements policy filters that constrain data structure and content to [*Assignment: organization-defined information security policy requirements*].

Enhancement Supplemental Guidance: Constraining file lengths, allowed enumerations, character sets, schemas, and other data object attributes reduces the range of potential malicious and/or unsanctioned content. Examples of constraints include ensuring that: (i) character data fields only contain printable ASCII; (ii) character data fields only contain alpha-numeric characters;

(iii) character data fields do not contain special characters; or (iv) maximum field sizes and file lengths are enforced based upon organization-defined security policy.

(15) The information system, when transferring information between different security domains, detects unsanctioned information and prohibits the transfer of such information in accordance with the security policy.

Enhancement Supplemental Guidance: Actions to support this enhancement include: checking all transferred information for malware, implementing dirty word list searches on transferred information, and applying the same protection measures to metadata (e.g., security attributes) that is applied to the information payload.

(16) The information system enforces security policies regarding information on interconnected systems.

Enhancement Supplemental Guidance: Transferring information between interconnected information systems of differing security policies introduces risk that such transfers violate one or more policies. While security policy violations may not be absolutely prohibited, policy guidance from information owners/stewards is implemented at the policy enforcement point between the interconnected systems. Specific architectural solutions are mandated, when required, to reduce the potential for undiscovered vulnerabilities. Architectural solutions include, for example: (i) prohibiting information transfers between interconnected systems (i.e. implementing access only, one way transfer mechanisms); (ii) employing hardware mechanisms to enforce unitary information flow directions; and (iii) implementing fully tested, re-grading mechanisms to reassign security attributes and associated security labels.

(17) The information system:

(a) Uniquely identifies and authenticates source and destination domains for information transfer;

(b) Binds security attributes to information to facilitate information flow policy enforcement; and

(c) Tracks problems associated with the security attribute binding and information transfer.

Enhancement Supplemental Guidance: Attribution is a critical component of a security concept of operations. The ability to identify source and destination points for information flowing in an information system, allows forensic reconstruction of events when required, and increases policy compliance by attributing policy violations to specific organizations/individuals. Means to enforce this enhancement include ensuring that the information system resolution labels distinguish between information systems and organizations, and between specific system components or individuals involved in preparing, sending, receiving, or disseminating information.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-4	**HIGH** AC-4

AC-5 SEPARATION OF DUTIES

Control: The organization:

a. Separates duties of individuals as necessary, to prevent malevolent activity without collusion;

b. Documents separation of duties; and

c. Implements separation of duties through assigned information system access authorizations.

Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. Related controls: AC-3.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-5	**HIGH** AC-5

AC-6 LEAST PRIVILEGE

Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Related controls: AC-2, AC-3, CM-7.

Control Enhancements:

(1) The organization explicitly authorizes access to [*Assignment: organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information*].

Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related control: AC-17.

(2) The organization requires that users of information system accounts, or roles, with access to [*Assignment: organization-defined list of security functions or security-relevant information*], use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.

Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of *role* is intended to address those situations where an access control policy such as *Role Based Access Control (RBAC)* is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.

(3) The organization authorizes network access to [*Assignment: organization-defined privileged commands*] only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

(4) The information system provides separate processing domains to enable finer-grained allocation of user privileges.

Enhancement Supplemental Guidance: Employing virtualization techniques to allow greater privilege within a virtual machine while restricting privilege to the underlying actual machine is an example of providing separate processing domains for finer-grained allocation of user privileges.

(5) The organization limits authorization to super user accounts on the information system to designated system administration personnel.

Enhancement Supplemental Guidance: Super user accounts are typically described as "root" or "administrator" for various types of commercial off-the-shelf operating systems. Configuring organizational information systems (e.g., notebook/laptop computers, servers, workstations) such that day-to-day users are not authorized access to super user accounts is an example of limiting system authorization. The organization may differentiate in the application of this control enhancement between allowed privileges for local information system accounts and for domain accounts provided the organization retains the ability to control the configuration of the system with regard to key security parameters and as otherwise necessary to sufficiently mitigate risk.

(6) The organization prohibits privileged access to the information system by non-organizational users.

Enhancement Supplemental Guidance: A qualified organizational user may be advised by a non-organizational user, if necessary.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** AC-6 (1) (2)	**HIGH** AC-6 (1) (2)

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

Control: The information system:

a. Enforces a limit of [*Assignment: organization-defined number*] consecutive invalid access attempts by a user during a [*Assignment: organization-defined time period*]; and

b. Automatically [*Selection: locks the account/node for an* [*Assignment: organization-defined time period*]; *locks the account/node until released by an administrator; delays next login prompt according to* [*Assignment: organization-defined delay algorithm*]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.

Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.

Control Enhancements:

(1) The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.

(2) The information system provides additional protection for mobile devices accessed via login by purging information from the device after [*Assignment: organization-defined number*] consecutive, unsuccessful login attempts to the device.

Enhancement Supplemental Guidance: This enhancement applies only to mobile devices for which a login occurs (e.g., personal digital assistants) and not to mobile devices accessed without a login such as removable media. In certain situations, this enhancement may not apply to mobile devices if the information on the device is encrypted with sufficiently strong encryption mechanisms, making purging unnecessary. The login is to the mobile device, not to any one account on the device. Therefore, a successful login to any account on the mobile device resets the unsuccessful login count to zero.

References: None.

Priority and Baseline Allocation:

P2	**LOW** AC-7	**MOD** AC-7	**HIGH** AC-7

AC-8 SYSTEM USE NOTIFICATION

Control: The information system:

a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;

b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and

c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.

Supplemental Guidance: System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-8	**MOD** AC-8	**HIGH** AC-8

AC-9 PREVIOUS LOGON (ACCESS) NOTIFICATION

Control: The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access).

Supplemental Guidance: This control is intended to cover both traditional logons to information systems and general accesses to information systems that occur in other types of architectural configurations (e.g., service oriented architectures).

Control Enhancements:

(1) The information system notifies the user, upon successful logon/access, of the number of unsuccessful logon/access attempts since the last successful logon/access.

(2) The information system notifies the user of the number of [*Selection: successful logins/accesses; unsuccessful login/access attempts; both*] during [*Assignment: organization-defined time period*].

(3) The information system notifies the user of [*Assignment: organization-defined set of security-related changes to the user's account*] during [*Assignment: organization-defined time period*].

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-10 CONCURRENT SESSION CONTROL

Control: The information system limits the number of concurrent sessions for each system account to [*Assignment: organization-defined number*].

Supplemental Guidance: The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AC-10

AC-11 SESSION LOCK

Control: The information system:

a. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.

Control Enhancements:

(1) The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.

References: OMB Memorandum 06-16.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** AC-11	**HIGH** AC-11

AC-12 SESSION TERMINATION

[Withdrawn: Incorporated into SC-10].

AC-13 SUPERVISION AND REVIEW — ACCESS CONTROL

[Withdrawn: Incorporated into AC-2 and AU-6].

AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

Control: The organization:

a. Identifies specific user actions that can be performed on the information system without identification or authentication; and

b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication.

Supplemental Guidance: This control is intended for those specific instances where an organization determines that no identification and authentication is required; it is not, however, mandating that such instances exist in given information system. The organization may allow a limited number of user actions without identification and authentication (e.g., when individuals access public websites or other publicly accessible federal information systems such as http://www.usa.gov). Organizations also identify any actions that normally require identification or authentication but may under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Such bypass may be, for example, via a software-readable physical switch that commands bypass of the login functionality and is protected from accidental or unmonitored use. This control does not apply to situations where identification and authentication have already occurred and are not being repeated, but rather to situations where identification and/or authentication have not yet occurred. Related control: CP-2, IA-2.

Control Enhancements:

(1) The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AC-14	**MOD** AC-14 (1)	**HIGH** AC-14 (1)

AC-15 AUTOMATED MARKING

[Withdrawn: Incorporated into MP-3].

AC-16 SECURITY ATTRIBUTES

Control: The information system supports and maintains the binding of [*Assignment: organization-defined security attributes*] to information in storage, in process, and in transmission.

Supplemental Guidance: Security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects and objects) with respect to safeguarding information. These attributes are typically associated with internal data structures (e.g., records, buffers, files) within the information system and are used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy. The term security label is often used to associate a set of security attributes with a specific information object as part of the data structure for that object (e.g., user access privileges, nationality, affiliation as contractor). Related controls: AC-3, AC-4, SC-16, MP-3.

Control Enhancements:

(1) **The information system dynamically reconfigures security attributes in accordance with an identified security policy as information is created and combined.**

(2) **The information system allows authorized entities to change security attributes.**

(3) **The information system maintains the binding of security attributes to information with sufficient assurance that the information--attribute association can be used as the basis for automated policy actions.**

Enhanced Supplemental Guidance: Examples of automated policy actions include automated access control decisions (e.g., Mandatory Access Control decisions), or decisions to release (or not release) information (e.g., information flows via cross domain systems).

(4) **The information system allows authorized users to associate security attributes with information.**

Enhanced Supplemental Guidance: The support provided by the information system can vary from prompting users to select security attributes to be associated with specific information objects, to ensuring that the combination of attributes selected is valid.

(5) **The information system displays security attributes in human-readable form on each object output from the system to system output devices to identify [*Assignment: organization-identified set of special dissemination, handling, or distribution instructions*] using [*Assignment: organization-identified human readable, standard naming conventions*].**

Enhancement Supplemental Guidance: Objects output from the information system include, for example, pages, screens, or equivalent. Output devices include, for example, printers and video displays on computer terminals, monitors, screens on notebook/laptop computers and personal digital assistants.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-17 REMOTE ACCESS

Control: The organization:

a. Documents allowed methods of remote access to the information system;

b. Establishes usage restrictions and implementation guidance for each allowed remote access method;

c. Monitors for unauthorized remote access to the information system;

d. Authorizes remote access to the information system prior to connection; and

e. Enforces requirements for remote connections to the information system.

Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization-controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.

Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.

(2) The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.

Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13.

(3) The information system routes all remote accesses through a limited number of managed access control points.

Enhancement Supplemental Guidance: Related control: SC-7.

(4) The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

Enhancement Supplemental Guidance: Related control: AC-6.

(5) The organization monitors for unauthorized remote connections to the information system [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.

(6) The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

(7) The organization ensures that remote sessions for accessing [*Assignment: organization-defined list of security functions and security-relevant information*] employ [*Assignment: organization-defined additional security measures*] and are audited.

Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.

(8) The organization disables [*Assignment: organization-defined networking protocols within the information system deemed to be nonsecure*] except for explicitly identified components in support of specific operational requirements.

Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

References: NIST Special Publications 800-46, 800-77, 800-113, 800-114, 800-121.

Priority and Baseline Allocation:

P1	**LOW** AC-17	**MOD** AC-17 (1) (2) (3) (4) (5) (7) (8)	**HIGH** AC-17 (1) (2) (3) (4) (5) (7) (8)

AC-18 WIRELESS ACCESS

Control: The organization:

a. Establishes usage restrictions and implementation guidance for wireless access;

b. Monitors for unauthorized wireless access to the information system;

c. Authorizes wireless access to the information system prior to connection; and

d. Enforces requirements for wireless connections to the information system.

Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization-controlled facilities. Related controls: AC-3, IA-2, IA-3, IA-8.

Control Enhancements:

(1) **The information system protects wireless access to the system using authentication and encryption.**

Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary. Related control: SC-13.

(2) **The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points [*Assignment: organization-defined frequency*], and takes appropriate action if an unauthorized connection is discovered.**

Enhancement Supplemental Guidance: Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.

(3) **The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.**

(4) **The organization does not allow users to independently configure wireless networking capabilities.**

(5) **The organization confines wireless communications to organization-controlled boundaries.**

Enhancement Supplemental Guidance: Actions that may be taken by the organization to confine wireless communications to organization-controlled boundaries include: (i) reducing the power of the wireless transmission such that it cannot transit the physical perimeter of the organization; (ii) employing measures such as TEMPEST to control wireless emanations; and (iii) configuring the wireless access such that it is point to point in nature.

References: NIST Special Publications 800-48, 800-94, 800-97.

Priority and Baseline Allocation:

P1	**LOW** AC-18	**MOD** AC-18 (1)	**HIGH** AC-18 (1) (2) (4) (5)

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

Control: The organization:

a. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;

b. Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;

c. Monitors for unauthorized connections of mobile devices to organizational information systems;

d. Enforces requirements for the connection of mobile devices to organizational information systems;

e. Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;

f. Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and

g. Applies [*Assignment: organization-defined inspection and preventative measures*] to mobile devices returning from locations that the organization deems to be of significant risk in accordance with organizational policies and procedures.

Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay.

Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.

Control Enhancements:

(1) The organization restricts the use of writable, removable media in organizational information systems.

(2) The organization prohibits the use of personally owned, removable media in organizational information systems.

(3) The organization prohibits the use of removable media in organizational information systems when the media has no identifiable owner.

Enhancement Supplemental Guidance: An identifiable owner (e.g., individual, organization, or project) for removable media helps to reduce the risk of using such technology by assigning responsibility and accountability for addressing known vulnerabilities in the media (e.g., malicious code insertion).

(4) The organization:

(a) Prohibits the use of unclassified mobile devices in facilities containing information systems processing, storing, or transmitting classified information unless specifically permitted by the appropriate authorizing official(s); and

(b) Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:

- **Connection of unclassified mobile devices to classified information systems is prohibited;**
- **Connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s);**
- **Use of internal or external modems or wireless interfaces within the mobile devices is prohibited; and**
- **Mobile devices and the information stored on those devices are subject to random reviews/inspections by [*Assignment: organization-defined security officials*], and if classified information is found, the incident handling policy is followed.**

References: NIST Special Publications 800-114, 800-124.

Priority and Baseline Allocation:

P1	**LOW** AC-19	**MOD** AC-19 (1) (2) (3)	**HIGH** AC-19 (1) (2) (3)

AC-20 USE OF EXTERNAL INFORMATION SYSTEMS

Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:

a. Access the information system from the external information systems; and

b. Process, store, and/or transmit organization-controlled information using the external information systems.

Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); (iii) information systems owned or controlled by nonfederal governmental organizations; and (iv) federal information systems that are not owned by, operated by, or under the direct supervision and authority of the organization. For some external systems, in particular those systems operated by other federal agencies, including organizations subordinate to those agencies, the trust relationships that have been established between those organizations and the originating organization may be such, that no explicit terms and conditions are required. In effect, the information systems of these organizations would not be considered external. These situations typically occur when, for example, there is some pre-existing sharing or trust agreement (either implicit or explicit) established between federal agencies and/or organizations subordinate to those agencies, or such trust agreements are specified by applicable laws, Executive Orders, directives, or policies. Authorized individuals include organizational personnel, contractors, or any other individuals with authorized access to the organizational information system and over which the organization has the authority to impose rules of behavior with regard to system access. The restrictions that an organization imposes on authorized individuals need not be uniform, as those restrictions are likely to vary depending upon the trust relationships between organizations. Thus, an organization might impose more stringent security restrictions on a contractor than on a state, local, or tribal government.

This control does not apply to the use of external information systems to access public interfaces to organizational information systems and information (e.g., individuals accessing federal information through www.usa.gov). The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.

Control Enhancements:

(1) The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:

(a) Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or

(b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system.

(2) The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.

Enhancement Supplemental Guidance: Limits on the use of organization-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** AC-20	**MOD** AC-20 (1) (2)	**HIGH** AC-20 (1) (2)

AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING

Control: The organization:

a. Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for [*Assignment: organization-defined information sharing circumstances where user discretion is required*]; and

b. Employs [*Assignment: list of organization-defined information sharing circumstances and automated mechanisms or manual processes required*] to assist users in making information sharing/collaboration decisions.

Supplemental Guidance: The control applies to information that may be restricted in some manner (e.g., privileged medical, contract-sensitive, proprietary, personally identifiable information, special access programs/compartments) based on some formal or administrative determination. Depending on the information-sharing circumstance, the sharing partner may be defined at the individual, group, or organization level and information may be defined by specific content, type, or security categorization. Related control: AC-3.

Control Enhancements:

(1) The information system employs automated mechanisms to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AC-22 PUBLICLY ACCESSIBLE CONTENT

Control: The organization:

a. Designates individuals authorized to post information onto an organizational information system that is publicly accessible;

b. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;

c. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;

d. Reviews the content on the publicly accessible organizational information system for nonpublic information [*Assignment: organization-defined frequency*]; and

e. Removes nonpublic information from the publicly accessible organizational information system, if discovered.

Supplemental Guidance: Nonpublic information is any information for which the general public is not authorized access in accordance with federal laws, Executive Orders, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by appropriate organizational policy. Related controls: AC-3, AU-13.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** AC-22	**MOD** AC-22	**HIGH** AC-22

FAMILY: AWARENESS AND TRAINING **CLASS:** OPERATIONAL

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AT-1	**MOD** AT-1	**HIGH** AT-1

AT-2 SECURITY AWARENESS

Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to the organization's information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

Control Enhancements:

(1) The organization includes practical exercises in security awareness training that simulate actual cyber attacks.

Enhancement Supplemental Guidance: Practical exercises may include, for example, no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking malicious web links.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publication 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-2	**MOD** AT-2	**HIGH** AT-2

AT-3 SECURITY TRAINING

Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [*Assignment: organization-defined frequency*] thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization’s information security program. Related controls: AT-2, SA-3.

Control Enhancements:

(1) **The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.**

Enhancement Supplemental Guidance: Environmental controls include, for example, fire suppression and detection devices/systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature/humidity, HVAC, and power within the facility.

(2) **The organization provides employees with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.**

Enhancement Supplemental Guidance: Physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring and surveillance equipment, and security guards (deployment and operating procedures).

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P1	**LOW** AT-3	**MOD** AT-3	**HIGH** AT-3

AT-4 SECURITY TRAINING RECORDS

Control: The organization:

a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and

b. Retains individual training records for [*Assignment: organization-defined time period*].

Supplemental Guidance: While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AT-4	**MOD** AT-4	**HIGH** AT-4

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:

- To facilitate ongoing security education and training for organizational personnel;
- To stay up to date with the latest recommended security practices, techniques, and technologies; and
- To share current security-related information including threats, vulnerabilities, and incidents.

Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization’s mission/business requirements. Information-sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: AUDIT AND ACCOUNTABILITY **CLASS:** TECHNICAL

AU-1 AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the audit and accountability family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The audit and accountability policy can be included as part of the general information security policy for the organization. Audit and accountability procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the audit and accountability policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** AU-1	**MOD** AU-1	**HIGH** AU-1

AU-2 AUDITABLE EVENTS

Control: The organization:

a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [*Assignment: organization-defined list of auditable events*];

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [*Assignment: organization-defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event*].

Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of *auditable* events that are to be *audited* at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Related control: AU-3.

Control Enhancements:

(1) [Withdrawn: Incorporated into AU-12].

(2) [Withdrawn: Incorporated into AU-12].

(3) **The organization reviews and updates the list of auditable events [*Assignment: organization-defined frequency*].**

Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.

(4) **The organization includes execution of privileged functions in the list of events to be audited by the information system.**

References: NIST Special Publication 800-92; Web: CSRC.NIST.GOV/PCIG/CIG.HTML.

Priority and Baseline Allocation:

P1	**LOW** AU-2	**MOD** AU-2 (3) (4)	**HIGH** AU-2 (3) (4)

AU-3 CONTENT OF AUDIT RECORDS

Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.

Control Enhancements:

(1) **The information system includes [*Assignment: organization-defined additional, more detailed information*] in the audit records for audit events identified by type, location, or subject.**

Enhancement Supplemental Guidance: An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.

(2) **The organization centrally manages the content of audit records generated by [*Assignment: organization-defined information system components*].**

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-3	**MOD** AU-3 (1)	**HIGH** AU-3 (1) (2)

AU-4 AUDIT STORAGE CAPACITY

Control: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.

Supplemental Guidance: The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7, SI-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-4	**MOD** AU-4	**HIGH** AU-4

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

Control: The information system:

a. Alerts designated organizational officials in the event of an audit processing failure; and

b. Takes the following additional actions: [*Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)*].

Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.

Control Enhancements:

(1) The information system provides a warning when allocated audit record storage volume reaches [*Assignment: organization-defined percentage*] of maximum audit record storage capacity.

(2) The information system provides a real-time alert when the following audit failure events occur: [*Assignment: organization-defined audit failure events requiring real-time alerts*].

(3) The information system enforces configurable traffic volume thresholds representing auditing capacity for network traffic and [*Selection: rejects or delays*] network traffic above those thresholds.

(4) The information system invokes a system shutdown in the event of an audit failure, unless an alternative audit capability exists.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-5	**MOD** AU-5	**HIGH** AU-5 (1) (2)

AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING

Control: The organization:

a. Reviews and analyzes information system audit records [*Assignment: organization-defined frequency*] for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and

b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Supplemental Guidance: Related control: AU-7.

Control Enhancements:

(1) **The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.**

(2) [Withdrawn: Incorporated into SI-4].

(3) **The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.**

(4) **The information system centralizes the review and analysis of audit records from multiple components within the system.**

Enhancement Supplemental Guidance: An example of an automated mechanism for centralized review and analysis is a Security Information Management (SIM) product. Related control: AU-2.

(5) **The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.**

Enhancement Supplemental Guidance: A Security Event/Information Management system tool can facilitate audit record aggregation and consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by the organization (with localized script adjustments, as necessary), provides a more cost-effective approach for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of the vulnerability scans and correlating attack detection events with scanning results. Related control: AU-7, RA-5, SI-4.

(6) **The organization correlates information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.**

Enhancement Supplemental Guidance: Related control: PE-6.

(7) **The organization specifies the permitted actions for each authorized information system process, role, and/or user in the audit and accountability policy.**

Enhancement Supplemental Guidance: Permitted actions for information system processes, roles, and/or users associated with the review, analysis, and reporting of audit records include, for example, read, write, append, and delete.

(8) **The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that are to result in alerts*].**

(9) **The organization performs, in a physically dedicated information system, full-text analysis of privileged functions executed.**

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-6	**MOD** AU-6	**HIGH** AU-6 (1)

AU-7 AUDIT REDUCTION AND REPORT GENERATION

Control: The information system provides an audit reduction and report generation capability.

Supplemental Guidance: An audit reduction and report generation capability provides support for near real-time audit review, analysis, and reporting requirements described in AU-6 and after-the-fact investigations of security incidents. Audit reduction and reporting tools do not alter original audit records. Related control: AU-6.

Control Enhancements:

(1) The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** AU-7 (1)	**HIGH** AU-7 (1)

AU-8 TIME STAMPS

Control: The information system uses internal system clocks to generate time stamps for audit records.

Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Related control: AU-3.

Control Enhancements:

(1) The information system synchronizes internal information system clocks [*Assignment: organization-defined frequency*] with [*Assignment: organization-defined authoritative time source*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-8	**MOD** AU-8 (1)	**HIGH** AU-8 (1)

AU-9 PROTECTION OF AUDIT INFORMATION

Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.

Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.

Control Enhancements:

(1) The information system produces audit records on hardware-enforced, write-once media.

(2) The information system backs up audit records [*Assignment: organization-defined frequency*] onto a different system or media than the system being audited.

(3) The information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools.

Enhancement Supplemental Guidance: An example of a cryptographic mechanism for the protection of integrity is the computation and application of a cryptographic-signed hash using asymmetric cryptography, protecting the confidentiality of the key used to generate the hash, and using the public key to verify the hash information.

(4) The organization:

(a) Authorizes access to management of audit functionality to only a limited subset of privileged users; and

(b) Protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions.

Enhancement Supplemental Guidance: Auditing may not be reliable when performed by the information system to which the user being audited has privileged access. The privileged user may inhibit auditing or modify audit records. This control enhancement helps mitigate this risk by requiring that privileged access be further defined between audit-related privileges and other privileges, thus, limiting the users with audit-related privileges. Reducing the risk of audit compromises by privileged users can also be achieved, for example, by performing audit activity on a separate information system or by using storage media that cannot be modified (e.g., write-once recording devices).

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-9	**MOD** AU-9	**HIGH** AU-9

AU-10 NON-REPUDIATION

Control: The information system protects against an individual falsely denying having performed a particular action.

Supplemental Guidance: Examples of particular actions taken by individuals include creating information, sending a message, approving information (e.g., indicating concurrence or signing a contract), and receiving a message. Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from an individual, or if an individual took specific actions (e.g., sending an email, signing a contract, approving a procurement request) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (e.g., digital signatures, digital message receipts).

Control Enhancements:

(1) The information system associates the identity of the information producer with the information.

Enhancement Supplemental Guidance: This control enhancement supports audit requirements that provide appropriate organizational officials the means to identify who produced specific information in the event of an information transfer. The nature and strength of the binding between the information producer and the information are determined and approved by the appropriate organizational officials based on the security categorization of the information and relevant risk factors.

(2) The information system validates the binding of the information producer's identity to the information.

Enhancement Supplemental Guidance: This control enhancement is intended to mitigate the risk that information is modified between production and review. The validation of bindings can be achieved, for example, by the use of cryptographic checksums.

(3) The information system maintains reviewer/releaser identity and credentials within the established chain of custody for all information reviewed or released.

Enhancement Supplemental Guidance: If the reviewer is a human or if the review function is automated but separate from the release/transfer function, the information system associates the identity of the reviewer of the information to be released with the information and the information label. In the case of human reviews, this control enhancement provides appropriate organizational officials the means to identify who reviewed and released the information. In the case of automated reviews, this control enhancement helps ensure that only approved review functions are employed.

(4) The information system validates the binding of the reviewer's identity to the information at the transfer/release point prior to release/transfer from one security domain to another security domain.

Enhancement Supplemental Guidance: This control enhancement is intended to mitigate the risk that information is modified between review and transfer/release.

(5) The organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.

Enhancement Supplemental Guidance: Related control: SC-13.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** AU-10

AU-11 AUDIT RECORD RETENTION

Control: The organization retains audit records for [*Assignment: organization-defined time period consistent with records retention policy*] to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The National Archives and Records Administration (NARA) General Records Schedules (GRS) provide federal policy on record retention.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** AU-11	**MOD** AU-11	**HIGH** AU-11

AU-12 AUDIT GENERATION

Control: The information system:

a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [*Assignment: organization-defined information system components*];

b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and

c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.

Supplemental Guidance: Audits records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). Related controls: AU-2, AU-3.

Control Enhancements:

(1) The information system compiles audit records from [*Assignment: organization-defined information system components*] into a system-wide (logical or physical) audit trail that is time-correlated to within [*Assignment: organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail*].

Enhancement Supplemental Guidance: The audit trail is time-correlated if the time stamp in the individual audit records can be reliably related to the time stamp in other audit records to achieve a time ordering of the records within the organization-defined tolerance.

(2) The information system produces a system-wide (logical or physical) audit trail composed of audit records in a standardized format.

Enhancement Supplemental Guidance: Audit information normalized to a common standard promotes interoperability and exchange of such information between dissimilar devices and information systems. This facilitates an audit system that produces event information that can be more readily analyzed and correlated. System log records and audit records compliant with the Common Event Expression (CEE) are examples of standard formats for audit records. If individual logging mechanisms within the information system do not conform to a standardized format, the system may convert individual audit records into a standardized format when compiling the system-wide audit trail.

References: None.

Priority and Baseline Allocation:

P1	**LOW** AU-12	**MOD** AU-12	**HIGH** AC-12 (1)

AU-13 MONITORING FOR INFORMATION DISCLOSURE

Control: The organization monitors open source information for evidence of unauthorized exfiltration or disclosure of organizational information [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

AU-14 SESSION AUDIT

Control: The information system provides the capability to:

a. Capture/record and log all content related to a user session; and

b. Remotely view/hear all content related to an established user session in real time.

Supplemental Guidance: Session auditing activities are developed, integrated, and used in consultation with legal counsel in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Control Enhancements:

(1) The information system initiates session audits at system start-up.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SECURITY ASSESSMENT AND AUTHORIZATION **CLASS:** MANAGEMENT

CA-1 SECURITY ASSESSMENT AND AUTHORIZATION POLICIES AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security assessment and authorization family. The policies and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security assessment/authorization policies can be included as part of the general information security policy for the organization. Security assessment/authorization procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security assessment and authorization policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-37, 800-53A, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CA-1	**MOD** CA-1	**HIGH** CA-1

CA-2 SECURITY ASSESSMENTS

Control: The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment;
- Assessment procedures to be used to determine security control effectiveness; and
- Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system [*Assignment: organization-defined frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

Supplemental Guidance: The organization assesses the security controls in an information system as part of: (i) security authorization or reauthorization; (ii) meeting the FISMA requirement for annual assessments; (iii) continuous monitoring; and (iv) testing/evaluation of the information system as part of the system development life cycle process. The assessment report documents the assessment results in sufficient detail as deemed necessary by the organization, to determine the accuracy and completeness of the report and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the information system. The FISMA requirement for (at least) annual security control assessments should *not* be interpreted by organizations as adding additional assessment requirements to those requirements already in place in the security authorization process. To satisfy the FISMA annual assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (i) assessments conducted as part of an information system authorization or reauthorization process; (ii) continuous monitoring (see CA-7); or (iii) testing and evaluation of an information system as part of the ongoing system development life cycle (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security control assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed.

Subsequent to the initial authorization of the information system and in accordance with OMB policy, the organization assesses a subset of the security controls annually during continuous monitoring. The organization establishes the security control selection criteria and subsequently selects a subset of the security controls within the information system and its environment of operation for assessment. Those security controls that are the most volatile (i.e., controls most affected by ongoing changes to the information system or its environment of operation) or deemed critical by the organization to protecting organizational operations and assets, individuals, other organizations, and the Nation are assessed more frequently in accordance with an organizational assessment of risk. All other controls are assessed at least once during the information system's three-year authorization cycle. The organization can use the current year's assessment results from any of the above sources to meet the FISMA annual assessment requirement provided that the results are current, valid, and relevant to determining security control effectiveness. External audits (e.g., audits conducted by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-6, CA-7, PM-9, SA-11.

Control Enhancements:

(1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system.

Enhancement Supplemental Guidance: An independent assessor or assessment team is any individual or group capable of conducting an impartial assessment of an organizational information system. Impartiality implies that the assessors are free from any perceived or actual conflicts of interest with respect to the developmental, operational, and/or management chain associated with the information system or to the determination of security control effectiveness. Independent security assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the impartiality of the assessor or assessment team conducting the assessment of the security controls in the information system. The authorizing official determines the required level of assessor independence based on the security categorization of the information system and/or the ultimate risk to organizational operations and assets, and to individuals. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a credible, risk-based decision. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, accuracy, integrity, and reliability of the results.

(2) The organization includes as part of security control assessments, [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises;* [*Assignment: organization-defined other forms of security testing*]].

Enhancement Supplemental Guidance: Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consists of: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Red team exercises are conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions. Information system monitoring, malicious user testing, penetration testing, red-team exercises, and other forms of security testing (e.g., independent verification and validation) are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. Testing is conducted in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Testing methods are approved by authorizing officials in coordination with the organization’s Risk Executive Function. Vulnerabilities uncovered during red team exercises are incorporated into the vulnerability remediation process. Related controls: RA-5, SI-2.

References: FIPS Publication 199; NIST Special Publications 800-37, 800-53A, 800-115.

Priority and Baseline Allocation:

P2	**LOW** CA-2	**MOD** CA-2 (1)	**HIGH** CA-2 (1) (2)

CA-3 INFORMATION SYSTEM CONNECTIONS

Control: The organization:

a. Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;

b. Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and

c. Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.

Supplemental Guidance: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between a federal agency and a nonfederal (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. Related controls: AC-4, IA-3, SC-7, SA-9.

Control Enhancements:

(1) The organization prohibits the direct connection of an unclassified, national security system to an external network.

Enhancement Supplemental Guidance: An external network is a network that is not controlled by the organization (e.g., the Internet). No direct connection means that an information system cannot connect to an external network without the use of an approved boundary protection device (e.g., firewall) that mediates the communication between the system and the network.

(2) The organization prohibits the direct connection of a classified, national security system to an external network.

Enhancement Supplemental Guidance: An external network is a network that is not controlled by the organization (e.g., the Internet). No direct connection means that an information system cannot connect to an external network without the use of an approved boundary protection device (e.g., firewall) that mediates the communication between the system and the network. In addition, the approved boundary protection device (typically a managed interface/cross-domain system), provides information flow enforcement from the information system to the external network consistent with AC-4.

References: FIPS Publication 199; NIST Special Publication 800-47.

Priority and Baseline Allocation:

P1	**LOW** CA-3	**MOD** CA-3	**HIGH** CA-3

CA-4 SECURITY CERTIFICATION

[Withdrawn: Incorporated into CA-2].

CA-5 PLAN OF ACTION AND MILESTONES

Control: The organization:

a. Develops a plan of action and milestones for the information system to document the organization’s planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and

b. Updates existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

Supplemental Guidance: The plan of action and milestones is a key document in the security authorization package and is subject to federal reporting requirements established by OMB. Related control: PM-4.

Control Enhancements:

(1) The organization employs automated mechanisms to help ensure that the plan of action and milestones for the information system is accurate, up to date, and readily available.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

Priority and Baseline Allocation:

P3	**LOW** CA-5	**MOD** CA-5	**HIGH** CA-5

CA-6 SECURITY AUTHORIZATION

Control: The organization:

a. Assigns a senior-level executive or manager to the role of authorizing official for the information system;

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and

c. Updates the security authorization [*Assignment: organization-defined frequency*].

Supplemental Guidance: Security authorization is the official management decision given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently federal responsibility and therefore, authorizing officials must be federal employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the information system owner with an up-to-date status of the security state of the information system. To reduce the administrative cost of security reauthorization, the authorizing official uses the results of the continuous monitoring process to the maximum extent possible as the basis for rendering a reauthorization decision. OMB policy requires that federal information systems are reauthorized at least every three years or when there is a significant change to the system. The organization defines what constitutes a significant change to the information system. Related controls: CA-2, CA-7, PM-9, PM-10.

Control Enhancements: None.

References: OMB Circular A-130; NIST Special Publication 800-37.

Priority and Baseline Allocation:

P3	**LOW** CA-6	**MOD** CA-6	**HIGH** CA-6

CA-7 CONTINUOUS MONITORING

Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

a. A configuration management process for the information system and its constituent components;

b. A determination of the security impact of changes to the information system and environment of operation;

c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and

d. Reporting the security state of the information system to appropriate organizational officials [*Assignment: organization-defined frequency*].

Supplemental Guidance: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the impact level of the information system. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4.

Control Enhancements:

(1) The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis.

Enhancement Supplemental Guidance: The organization can extend and maximize the value of the ongoing assessment of security controls during the continuous monitoring process by requiring an independent assessor or team to assess all of the security controls during the information system's three-year authorization cycle. See supplemental guidance for CA-2, enhancement (1), for further information on assessor independence. Related controls: CA-2, CA-5, CA-6, CM-4.

(2) The organization plans, schedules, and conducts assessments [*Assignment: organization-defined frequency*], [*Selection: announced; unannounced*], [*Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises;* [*Assignment: organization-defined other forms of security assessment*]] to ensure compliance with all vulnerability mitigation procedures.

Enhancement Supplemental Guidance: Examples of vulnerability mitigation procedures are contained in Information Assurance Vulnerability Alerts. Testing is intended to ensure that the information system continues to provide adequate security against constantly evolving threats and vulnerabilities. Conformance testing also provides independent validation. See supplemental guidance for CA-2, enhancement (2) for further information on malicious user testing, penetration testing, red-team exercises, and other forms of security testing. Related control: CA-2.

References: NIST Special Publications 800-37, 800-53A; US-CERT Technical Cyber Security Alerts; DOD Information Assurance Vulnerability Alerts.

Priority and Baseline Allocation:

P3	**LOW** CA-7	**MOD** CA-7	**HIGH** CA-7

FAMILY: CONFIGURATION MANAGEMENT **CLASS:** OPERATIONAL

CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the configuration management family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The configuration management policy can be included as part of the general information security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the configuration management policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CM-1	**MOD** CM-1	**HIGH** CM-1

CM-2 BASELINE CONFIGURATION

Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9.

Control Enhancements:

(1) The organization reviews and updates the baseline configuration of the information system:

(a) [*Assignment: organization-defined frequency*];

(b) When required due to [*Assignment organization-defined circumstances*]; and

(c) As an integral part of information system component installations and upgrades.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

Enhancement Supplemental Guidance: Software inventory tools are examples of automated mechanisms that help organizations maintain consistent baseline configurations for information systems. Software inventory tools can be deployed for each operating system in use within the organization (e.g., on workstations, servers, network components, mobile devices) and used to track operating system version numbers, applications and types of software installed on the operating systems, and current patch levels. Software inventory tools can also scan information systems for unauthorized software to validate organization-defined lists of authorized and unauthorized software programs.

(3) The organization retains older versions of baseline configurations as deemed necessary to support rollback.

(4) The organization:

(a) Develops and maintains [*Assignment: organization-defined list of software programs not authorized to execute on the information system*]; and

(b) Employs an allow-all, deny-by-exception authorization policy to identify software allowed to execute on the information system.

(5) The organization:

(a) Develops and maintains [*Assignment: organization-defined list of software programs authorized to execute on the information system*]; and

(b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.

(6) The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-2	**MOD** CM-2 (1) (3) (4)	**HIGH** CM-2 (1) (2) (3) (5) (6)

CM-3 CONFIGURATION CHANGE CONTROL

Control: The organization:

a. Determines the types of changes to the information system that are configuration controlled;

b. Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;

c. Documents approved configuration-controlled changes to the system;

d. Retains and reviews records of configuration-controlled changes to the system;

e. Audits activities associated with configuration-controlled changes to the system; and

f. Coordinates and provides oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element (e.g., committee, board*] that convenes [*Selection: (one or more):* [*Assignment: organization-defined frequency*]; [*Assignment: organization-defined configuration change conditions*]].

Supplemental Guidance: The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered

Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. Related controls: CM-4, CM-5, CM-6, SI-2.

Control Enhancements:

(1) The organization employs automated mechanisms to:

(a) Document proposed changes to the information system;

(b) Notify designated approval authorities;

(c) Highlight approvals that have not been received by [*Assignment: organization-defined time period*];

(d) Inhibit change until designated approvals are received; and

(e) Document completed changes to the information system.

(2) The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.

Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.

(3) The organization employs automated mechanisms to implement changes to the current information system baseline and deploys the updated baseline across the installed base.

Enhancement Supplemental Guidance: Related controls: CM-2, CM-6.

(4) The organization requires an information security representative to be a member of the [*Assignment: organization-defined configuration change control element (e.g., committee, board)*].

Enhancement Supplemental Guidance: Information security representatives can include, for example, information system security officers or information system security managers. The configuration change control element in this control enhancement is consistent with the change control element defined by the organization in CM-3.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-3 (2)	**HIGH** CM-3 (1) (2)

CM-4 SECURITY IMPACT ANALYSIS

Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.

Supplemental Guidance: Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the impact level of the information system. Related controls: CA-2, CA-7, CM-3, CM-9, SI-2.

Control Enhancements:

(1) The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.

(2) The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.

Enhancement Supplemental Guidance: Changes include information system upgrades and modifications.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P2	**LOW** CM-4	**MOD** CM-4	**HIGH** CM-4 (1)

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.

Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes. Related controls: AC-3, AC-6, PE-3.

Control Enhancements:

(1) The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.

(2) The organization conducts audits of information system changes [*Assignment: organization-defined frequency*] and when indications so warrant to determine whether unauthorized changes have occurred.

(3) The information system prevents the installation of [*Assignment: organization-defined critical software programs*] that are not signed with a certificate that is recognized and approved by the organization.

Enhancement Supplemental Guidance: Critical software programs and/or modules include, for example, patches, service packs, and where applicable, device drivers.

(4) The organization enforces a two-person rule for changes to [*Assignment: organization-defined information system components and system-level information*].

(5) The organization:

(a) Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and

(b) Reviews and reevaluates information system developer/integrator privileges [*Assignment: organization-defined frequency*].

(6) The organization limits privileges to change software resident within software libraries (including privileged programs).

(7) The information system automatically implements [*Assignment: organization-defined safeguards and countermeasures*] if security functions (or mechanisms) are changed inappropriately.

Enhancement Supplemental Guidance: The information system reacts automatically when inappropriate and/or unauthorized modifications have occurred to security functions or mechanisms. Automatic implementation of safeguards and countermeasures includes, for example, reversing the change, halting the information system or triggering an audit alert when an unauthorized modification to a critical security file occurs.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-5	**HIGH** CM-5 (1) (2) (3)

CM-6 CONFIGURATION SETTINGS

Control: The organization:

a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;

b. Implements the configuration settings;

c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and

d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Supplemental Guidance: Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A *security configuration checklist* (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, federal agencies (and other government organizations), and others in the public and private sectors. An example of a security configuration checklist is the Federal Desktop Core Configuration (FDCC) which potentially affects the implementation of CM-6 and other controls such as AC-19 and CM-7. The Security Content Automation Protocol (SCAP) and defined standards within the protocol (e.g., Common Configuration Enumeration) provide an effective method to uniquely identify, track, and control configuration settings. OMB establishes federal policy on configuration requirements for federal information systems. Related controls: CM-2, CM-3, SI-4.

Control Enhancements:

(1) The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings.

(2) The organization employs automated mechanisms to respond to unauthorized changes to [*Assignment: organization-defined configuration settings*].

Enhancement Supplemental Guidance: Responses to unauthorized changes to configuration settings can include, for example, alerting designated organizational personnel, restoring mandatory/organization-defined configuration settings, or in the extreme case, halting affected information system processing.

(3) The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.

Enhancement Supplemental Guidance: Related controls: IR-4, IR-5.

(4) The information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance (i.e., security checklists), prior to being introduced into a production environment.

References: OMB Memoranda 07-11, 07-18, 08-22; NIST Special Publications 800-70, 800-128; Web: NVD.NIST.GOV; WWW.NSA.GOV.

Priority and Baseline Allocation:

P1	**LOW** CM-6	**MOD** CM-6 (3)	**HIGH** CM-6 (1) (2) (3)

CM-7 LEAST FUNCTIONALITY

Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [*Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services*].

Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component. Where feasible, organizations limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related control: RA-5.

Control Enhancements:

(1) The organization reviews the information system [*Assignment: organization-defined frequency*] to identify and eliminate unnecessary functions, ports, protocols, and/or services.

(2) The organization employs automated mechanisms to prevent program execution in accordance with [*Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage*].

Enhancement Supplemental Guidance: Related control: CM-2.

(3) The organization ensures compliance with [*Assignment: organization-defined registration requirements for ports, protocols, and services*].

Enhancement Supplemental Guidance: Organizations use the registration process to manage, track, and provide oversight for information systems and implemented functionality.

References: None.

Priority and Baseline Allocation:

P1	**LOW** CM-7	**MOD** CM-7 (1)	**HIGH** CM-7 (1) (2)

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Control: The organization develops, documents, and maintains an inventory of information system components that:

a. Accurately reflects the current information system;

b. Is consistent with the authorization boundary of the information system;

c. Is at the level of granularity deemed necessary for tracking and reporting;

d. Includes [*Assignment: organization-defined information deemed necessary to achieve effective property accountability*]; and

e. Is available for review and audit by designated organizational officials.

Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. Related controls: CM-2, CM-6.

Control Enhancements:

(1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

(2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Enhancement Supplemental Guidance: Organizations maintain the information system inventory to the extent feasible. Virtual machines, for example, can be difficult to monitor because they are not visible to the network when not in use. In such cases, the intent of this control enhancement is to maintain as up-to-date, complete, and accurate an inventory as is reasonable.

(3) The organization:

(a) Employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the addition of unauthorized components/devices into the information system; and

(b) Disables network access by such components/devices or notifies designated organizational officials.

Enhancement Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections in AC-17 and for unauthorized mobile devices in AC-19. The monitoring for unauthorized components/devices on information system networks may be accomplished on an ongoing basis or by the periodic scanning of organizational networks for that purpose. Automated mechanisms can be implemented within the information system and/or in another separate information system or device. Related controls: AC-17, AC-19.

(4) The organization includes in property accountability information for information system components, a means for identifying by [*Selection (one or more): name; position; role*] individuals responsible for administering those components.

(5) The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.

(6) The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.

Enhancement Supplemental Guidance: This control enhancement focuses on the configuration settings established by the organization for its information system components, the specific information system components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings in the deployed information system components. Related controls: CM-2, CM-6.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** CM-8	**MOD** CM-8 (1) (5)	**HIGH** CM-8 (1) (2) (3) (4) (5)

CM-9 CONFIGURATION MANAGEMENT PLAN

Control: The organization develops, documents, and implements a configuration management plan for the information system that:

a. Addresses roles, responsibilities, and configuration management processes and procedures;

b. Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and

c. Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.

Supplemental Guidance: Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization’s configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system. Related control: SA-10.

Control Enhancements:

(1) The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.

Enhancement Supplemental Guidance: In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process.

References: NIST Special Publication 800-128.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CM-9	**HIGH** CM-9

FAMILY: CONTINGENCY PLANNING **CLASS:** OPERATIONAL

CP-1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the contingency planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The contingency planning policy can be included as part of the general information security policy for the organization. Contingency planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the contingency planning policy. Related control: PM-9.

Control Enhancements: None.

References: Federal Continuity Directive 1; NIST Special Publications 800-12, 800-34, 800-100.

Priority and Baseline Allocation:

P1	**LOW** CP-1	**MOD** CP-1	**HIGH** CP-1

CP-2 CONTINGENCY PLAN

Control: The organization:

a. Develops a contingency plan for the information system that:

- Identifies essential missions and business functions and associated contingency requirements;
- Provides recovery objectives, restoration priorities, and metrics;
- Addresses contingency roles, responsibilities, assigned individuals with contact information;
- Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;
- Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and
- Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the contingency plan to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*];

c. Coordinates contingency planning activities with incident handling activities;

d. Reviews the contingency plan for the information system [*Assignment: organization-defined frequency*];

e. Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and

f. Communicates contingency plan changes to [*Assignment: organization-defined list of key contingency personnel (identified by name and/or by role) and organizational elements*].

Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, Executive Orders, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Related controls: AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.

Control Enhancements:

(1) The organization coordinates contingency plan development with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

(2) The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.

(3) The organization plans for the resumption of essential missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

(4) The organization plans for the full resumption of missions and business functions within [*Assignment: organization-defined time period*] of contingency plan activation.

(5) The organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full information system restoration at primary processing and/or storage sites.

(6) The organization provides for the transfer of all essential missions and business functions to alternate processing and/or storage sites with little or no loss of operational continuity and sustains that continuity through restoration to primary processing and/or storage sites.

References: Federal Continuity Directive 1; NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-2	**MOD** CP-2 (1)	**HIGH** CP-2 (1) (2) (3)

CP-3 CONTINGENCY TRAINING

Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training [*Assignment: organization-defined frequency*].

Supplemental Guidance: None.

Control Enhancements:

(1) The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

References: NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** CP-3	**MOD** CP-3	**HIGH** CP-3 (1)

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

Control: The organization:

a. Tests and/or exercises the contingency plan for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the plan's effectiveness and the organization's readiness to execute the plan; and

b. Reviews the contingency plan test/exercise results and initiates corrective actions.

Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.

Control Enhancements:

(1) The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.

Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.

(2) The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.

(3) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the contingency plan by providing more complete coverage of contingency issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the information system and supported missions.

(4) The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.

Enhancement Supplemental Guidance: Related controls: CP-10, SC-24.

References: FIPS Publication 199; NIST Special Publications 800-34, 800-84.

Priority and Baseline Allocation:

P2	**LOW** CP-4	**MOD** CP-4 (1)	**HIGH** CP-4 (1) (2) (4)

CP-5 CONTINGENCY PLAN UPDATE

[Withdrawn: Incorporated into CP-2].

CP-6 ALTERNATE STORAGE SITE

Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.

Supplemental Guidance: Related controls: CP-2, CP-9, MP-4.

Control Enhancements:

(1) The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.

Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.

(2) The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.

(3) The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

Enhancement Supplemental Guidance: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-6 (1) (3)	**HIGH** CP-6 (1) (2) (3)

CP-7 ALTERNATE PROCESSING SITE

Control: The organization:

a. Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period consistent with recovery time objectives*] when the primary processing capabilities are unavailable; and

b. Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

(1) The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.

Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.

(2) The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.

(3) The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.

(4) The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.

(5) The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-7 (1) (2) (3) (5)	**HIGH** CP-7 (1) (2) (3) (4) (5)

CP-8 TELECOMMUNICATIONS SERVICES

Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [*Assignment: organization-defined time period*] when the primary telecommunications capabilities are unavailable.

Supplemental Guidance: Related control: CP-2.

Control Enhancements:

(1) The organization:

(a) Develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with the organization’s availability requirements; and

(b) Requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.

(2) The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.

(3) The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.

(4) The organization requires primary and alternate telecommunications service providers to have contingency plans.

References: NIST Special Publication 800-34; Web: TSP.NCS.GOV.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** CP-8 (1) (2)	**HIGH** CP-8 (1) (2) (3) (4)

CP-9 INFORMATION SYSTEM BACKUP

Control: The organization:

a. Conducts backups of user-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

b. Conducts backups of system-level information contained in the information system [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*];

c. Conducts backups of information system documentation including security-related documentation [*Assignment: organization-defined frequency consistent with recovery time and recovery point objectives*]; and

d. Protects the confidentiality and integrity of backup information at the storage location.

Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4.

Control Enhancements:

(1) **The organization tests backup information [*Assignment: organization-defined frequency*] to verify media reliability and information integrity.**

(2) **The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.**

(3) **The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not colocated with the operational system.**

(4) [Withdrawn: Incorporated into CP-9].

(5) **The organization transfers information system backup information to the alternate storage site [*Assignment: organization-defined time period and transfer rate consistent with the recovery time and recovery point objectives*].**

(6) **The organization accomplishes information system backup by maintaining a redundant secondary system, not collocated, that can be activated without loss of information or disruption to the operation.**

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-9	**MOD** CP-9 (1)	**HIGH** CP-9 (1) (2) (3)

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

Supplemental Guidance: Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, SC-24.

Control Enhancements:

(1) [Withdrawn: Incorporated into CP-4].

(2) **The information system implements transaction recovery for systems that are transaction-based.**

Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.

(3) **The organization provides compensating security controls for [*Assignment: organization-defined circumstances that can inhibit recovery and reconstitution to a known state*].**

(4) **The organization provides the capability to reimage information system components within [*Assignment: organization-defined restoration time-periods*] from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.**

(5) **The organization provides [*Selection: real-time; near-real-time*] [*Assignment: organization-defined failover capability for the information system*].**

Enhancement Supplemental Guidance: Examples of failover capability are incorporating mirrored information system operations at an alternate processing site or periodic data mirroring at regular intervals during a time period defined by the organization's recovery time period.

(6) The organization protects backup and restoration hardware, firmware, and software.

Enhancement Supplemental Guidance: Protection of backup and restoration hardware, firmware, and software includes both physical and technical measures. Router tables, compilers, and other security-relevant system software are examples of backup and restoration software.

References: NIST Special Publication 800-34.

Priority and Baseline Allocation:

P1	**LOW** CP-10	**MOD** CP-10 (2) (3)	**HIGH** CP-10 (2) (3) (4)

FAMILY: IDENTIFICATION AND AUTHENTICATION **CLASS:** TECHNICAL

IA-1 IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the identification and authentication family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The identification and authentication policy can be included as part of the general information security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the identification and authentication policy. Related control: PM-9.

Control Enhancements: None.

References: FIPS Publication 201; NIST Special Publications 800-12, 800-63, 800-73, 800-76, 800-78, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IA-1	**MOD** IA-1	**HIGH** IA-1

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8.

The identification and authentication requirements in this control are satisfied by complying with Homeland Security Presidential Directive 12 consistent with organization-specific implementation plans provided to OMB. In addition to identifying and authenticating users at the information-system level (i.e., at logon), identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the organization. Related controls: AC-14, AC-17, AC-18, IA-4, IA-5.

Control Enhancements:

(1) The information system uses multifactor authentication for network access to privileged accounts.

(2) The information system uses multifactor authentication for network access to non-privileged accounts.

(3) The information system uses multifactor authentication for local access to privileged accounts.

(4) The information system uses multifactor authentication for local access to non-privileged accounts.

(5) The organization:

(a) Allows the use of group authenticators only when used in conjunction with an individual/unique authenticator; and

(b) Requires individuals to be authenticated with an individual authenticator prior to using a group authenticator.

(6) The information system uses multifactor authentication for network access to privileged accounts where one of the factors is provided by a device separate from the information system being accessed.

(7) The information system uses multifactor authentication for network access to non-privileged accounts where one of the factors is provided by a device separate from the information system being accessed.

(8) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to privileged accounts.

Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

(9) The information system uses [*Assignment: organization-defined replay-resistant authentication mechanisms*] for network access to non-privileged accounts.

Enhancement Supplemental Guidance: An authentication process resists replay attacks if it is impractical to achieve a successful authentication by recording and replaying a previous authentication message. Techniques used to address this include protocols that use nonces or challenges (e.g., TLS), and time synchronous or challenge-response one-time authenticators.

References: HSPD 12; OMB Memorandum 04-04; FIPS Publication 201; NIST Special Publications 800-63, 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

P1	**LOW** IA-2 (1)	**MOD** IA-2 (1) (2) (3) (8)	**HIGH** IA-2 (1) (2) (3) (4) (8) (9)

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined list of specific and/or types of devices*] before establishing a connection.

Supplemental Guidance: The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. The information system typically uses either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for identification or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the security categorization of the information system.

Control Enhancements:

(1) The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based.

Enhancement Supplemental Guidance: Remote network connection is any connection with a device communicating through an external network (e.g., the Internet). Related controls: AC-17, AC-18.

(2) The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.

(3) The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device.

Enhancement Supplemental Guidance: With regard to dynamic address allocation for devices, DHCP-enabled clients typically obtain *leases* for IP addresses from DHCP servers.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** IA-3	**HIGH** IA-3

IA-4 IDENTIFIER MANAGEMENT

Control: The organization manages information system identifiers for users and devices by:

a. Receiving authorization from a designated organizational official to assign a user or device identifier;

b. Selecting an identifier that uniquely identifies an individual or device;

c. Assigning the user identifier to the intended party or the device identifier to the intended device;

d. Preventing reuse of user or device identifiers for [*Assignment: organization-defined time period*]; and

e. Disabling the user identifier after [*Assignment: organization-defined time period of inactivity*].

Supplemental Guidance: Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). Related control: AC-2, IA-2.

Control Enhancements:

(1) **The organization prohibits the use of information system account identifiers as public identifiers for user electronic mail accounts (i.e., user identifier portion of the electronic mail address).**

Enhancement Supplemental Guidance: The organization implements this control enhancement to the extent that the information system allows.

(2) **The organization requires that registration to receive a user ID and password include authorization by a supervisor, and be done in person before a designated registration authority.**

(3) **The organization requires multiple forms of certification of individual identification such as documentary evidence or a combination of documents and biometrics be presented to the registration authority.**

(4) **The organization manages user identifiers by uniquely identifying the user as [*Assignment: organization-defined characteristic identifying user status*].**

Enhancement Supplemental Guidance: Characteristics identifying user status include, for example, contractors and foreign nationals.

(5) **The information system dynamically manages identifiers, attributes, and associated access authorizations.**

Enhancement Supplemental Guidance: In contrast to conventional approaches to identification and authentication which employ static information system accounts for preregistered users, many service-oriented architecture implementations rely on establishing identities at run time for entities that were previously unknown. Dynamic establishment of identities and association of attributes and privileges with these identities is anticipated and provisioned. Pre-established trust relationships and mechanisms with appropriate authorities to validate identities and related credentials are essential.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78.

Priority and Baseline Allocation:

P1	**LOW** IA-4	**MOD** IA-4	**HIGH** IA-4

IA-5 AUTHENTICATOR MANAGEMENT

Control: The organization manages information system authenticators for users and devices by:

a. Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;

b. Establishing initial authenticator content for authenticators defined by the organization;

c. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;

e. Changing default content of authenticators upon information system installation;

f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);

g. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];

h. Protecting authenticator content from unauthorized disclosure and modification; and

i. Requiring users to take, and having devices implement, specific measures to safeguard authenticators.

Supplemental Guidance: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.

Control Enhancements:

(1) **The information system, for password-based authentication:**

(a) **Enforces minimum password complexity of [*Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type*];**

(b) **Enforces at least a [*Assignment: organization-defined number of changed characters*] when new passwords are created;**

(c) **Encrypts passwords in storage and in transmission;**

(d) **Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and**

(e) **Prohibits password reuse for [Assignment: organization-defined number] generations.**

Enhancement Supplemental Guidance: This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does *not* apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.

(2) **The information system, for PKI-based authentication:**

(a) **Validates certificates by constructing a certification path with status information to an accepted trust anchor;**

(b) **Enforces authorized access to the corresponding private key; and**

(c) **Maps the authenticated identity to the user account.**

Enhancement Supplemental Guidance: Status information for certification paths includes, for example, certificate revocation lists or online certificate status protocol responses.

(3) **The organization requires that the registration process to receive [*Assignment: organization-defined types of and/or specific authenticators*] be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).**

(4) **The organization employs automated tools to determine if authenticators are sufficiently strong to resist attacks intended to discover or otherwise compromise the authenticators.**

(5) **The organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery.**

Enhancement Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation, by requiring vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators for those components prior to delivery to the organization. Unique authenticators are assigned by vendors and/or manufacturers to specific information system components (i.e., delivered information technology products) with distinct serial numbers. This requirement is included in acquisition documents prepared by the organization when procuring information systems and/or information system components.

(6) The organization protects authenticators commensurate with the classification or sensitivity of the information accessed.

(7) The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.

Enhancement Supplemental Guidance: Organizations exercise caution in determining whether an embedded or stored authenticator is in encrypted or unencrypted form. If the authenticator in its stored representation, is used in the manner stored, then that representation is considered an unencrypted authenticator. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).

(8) The organization takes [*Assignment: organization-defined measures*] to manage the risk of compromise due to individuals having accounts on multiple information systems.

Enhancement Supplemental Guidance: When an individual has accounts on multiple information systems, there is the risk that if one account is compromised and the individual is using the same user identifier and authenticator, other accounts will be compromised as well. Possible alternatives include, but are not limited to: (i) having the same user identifier but different authenticators on all systems; (ii) having different user identifiers and authenticators on each system; (iii) employing some form of single sign-on mechanism; or (iv) including some form of one-time passwords on all systems.

References: OMB Memorandum 04-04; FIPS Publication 201; NIST Special Publications 800-73, 800-63, 800-76, 800-78.

Priority and Baseline Allocation:

P1	**LOW** IA-5 (1)	**MOD** IA-5 (1) (2) (3)	**HIGH** IA-5 (1) (2) (3)

IA-6 AUTHENTICATOR FEEDBACK

Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** IA-6	**MOD** IA-6	**HIGH** IA-6

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Supplemental Guidance: None.

Control Enhancements: None.

References: FIPS Publication 140-2; Web: CSRC.NIST.GOV/CRYPTVAL.

Priority and Baseline Allocation:

P1	**LOW** IA-7	**MOD** IA-7	**HIGH** IA-7

IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)

Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).

Supplemental Guidance: Non-organizational users include all information system users other than organizational users explicitly covered by IA-2. Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in accordance with AC-14. In accordance with the E-Authentication E-Government initiative, authentication of non-organizational users accessing federal information systems may be required to protect federal, proprietary, or privacy-related information (with exceptions noted for national security systems). Accordingly, a risk assessment is used in determining the authentication needs of the organization. Scalability, practicality, and security are simultaneously considered in balancing the need to ensure ease of use for access to federal information and information systems with the need to protect and adequately mitigate risk to organizational operations, organizational assets, individuals, other organizations, and the Nation. Identification and authentication requirements for information system access by organizational users are described in IA-2. Related controls: AC-14, AC-17, AC-18, MA-4.

Control Enhancements: None.

References: OMB Memorandum 04-04; Web: WWW.CIO.GOV/EAUTHENTICATION; NIST Special Publication 800-63.

Priority and Baseline Allocation:

P1	**LOW** IA-8	**MOD** IA-8	**HIGH** IA-8

FAMILY: INCIDENT RESPONSE **CLASS:** OPERATIONAL

IR-1 INCIDENT RESPONSE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the incident response family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the incident response policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-61, 800-83, 800-100.

Priority and Baseline Allocation:

P1	**LOW** IR-1	**MOD** IR-1	**HIGH** IR-1

IR-2 INCIDENT RESPONSE TRAINING

Control: The organization:

a. Trains personnel in their incident response roles and responsibilities with respect to the information system; and

b. Provides refresher training [*Assignment: organization-defined frequency*].

Supplemental Guidance: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.

Control Enhancements:

(1) The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.

(2) The organization employs automated mechanisms to provide a more thorough and realistic training environment.

References: NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

P2	**LOW** IR-2	**MOD** IR-2	**HIGH** IR-2 (1) (2)

IR-3 INCIDENT RESPONSE TESTING AND EXERCISES

Control: The organization tests and/or exercises the incident response capability for the information system [*Assignment: organization-defined frequency*] using [*Assignment: organization-defined tests and/or exercises*] to determine the incident response effectiveness and documents the results.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability.

Enhancement Supplemental Guidance: Automated mechanisms can provide the ability to more thoroughly and effectively test or exercise the incident response capability by providing more complete coverage of incident response issues, selecting more realistic test/exercise scenarios and environments, and more effectively stressing the response capability. Related control: AT-2.

References: NIST Special Publications 800-84, 800-115.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** IR-3	**HIGH** IR-3 (1)

IR-4 INCIDENT HANDLING

Control: The organization:

a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;

b. Coordinates incident handling activities with contingency planning activities; and

c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.

Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.

Control Enhancements:

(1) The organization employs automated mechanisms to support the incident handling process.

Enhancement Supplemental Guidance: An online incident management system is an example of an automated mechanism.

(2) The organization includes dynamic reconfiguration of the information system as part of the incident response capability.

Enhancement Supplemental Guidance: Dynamic reconfiguration includes, for example, changes to router rules, access control lists, intrusion detection/prevention system parameters, and filter rules for firewalls and gateways.

(3) The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions.

Enhancement Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions that may be appropriate include, for example, graceful degradation, information system shutdown, fall back to manual mode or alternative technology whereby the system operates differently, employing deceptive measures (e.g., false data flows, false status measures), alternate information flows, or operating in a mode that is reserved solely for when a system is under attack.

(4) The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.

(5) The organization implements a configurable capability to automatically disable the information system if any of the following security violations are detected: [*Assignment: organization-defined list of security violations*].

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-4	**MOD** IR-4 (1)	**HIGH** IR-4 (1)

IR-5 INCIDENT MONITORING

Control: The organization tracks and documents information system security incidents.

Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.

Enhancement Supplemental Guidance: Automated mechanisms for tracking security incidents and collecting/analyzing incident information include, for example, the Einstein network monitoring device and monitoring online Computer Incident Response Centers (CIRCs) or other electronic databases of incidents. Related controls: AU-6, AU-7, SI-4.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-5	**MOD** IR-5	**HIGH** IR-5 (1)

IR-6 INCIDENT REPORTING

Control: The organization:

a. Requires personnel to report suspected security incidents to the organizational incident response capability within [*Assignment: organization-defined time-period*]; and

b. Reports security incident information to designated authorities.

Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for federal agencies and their subordinate organizations. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Current federal policy requires that all federal agencies (unless specifically exempted from such requirements) report security incidents to the United States Computer Emergency Readiness Team (US-CERT) within specified time frames designated in the US-CERT Concept of Operations for Federal Cyber Security Incident Handling. Related controls: IR-4, IR-5.

Control Enhancements:

(1) The organization employs automated mechanisms to assist in the reporting of security incidents.

(2) The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.

References: NIST Special Publication 800-61: Web: WWW.US-CERT.GOV.

Priority and Baseline Allocation:

P1	**LOW** IR-6	**MOD** IR-6 (1)	**HIGH** IR-6 (1)

IR-7 INCIDENT RESPONSE ASSISTANCE

Control: The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.

Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.

Control Enhancements:

(1) The organization employs automated mechanisms to increase the availability of incident response-related information and support.

Enhancement Supplemental Guidance: Automated mechanisms can provide a push and/or pull capability for users to obtain incident response assistance. For example, individuals might have access to a website to query the assistance capability, or conversely, the assistance capability may have the ability to proactively send information to users (general distribution or targeted) as part of increasing understanding of current response capabilities and support.

(2) The organization:

(a) Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and

(b) Identifies organizational incident response team members to the external providers.

Enhancement Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.

References: None.

Priority and Baseline Allocation:

P3	**LOW** IR-7	**MOD** IR-7 (1)	**HIGH** IR-7 (1)

IR-8 INCIDENT RESPONSE PLAN

Control: The organization:

a. Develops an incident response plan that:

- Provides the organization with a roadmap for implementing its incident response capability;
- Describes the structure and organization of the incident response capability;

- Provides a high-level approach for how the incident response capability fits into the overall organization;
- Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
- Defines reportable incidents;
- Provides metrics for measuring the incident response capability within the organization.
- Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
- Is reviewed and approved by designated officials within the organization;

b. Distributes copies of the incident response plan to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*];

c. Reviews the incident response plan [*Assignment: organization-defined frequency*];

d. Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and

e. Communicates incident response plan changes to [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role) and organizational elements*].

Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization’s mission, strategies, and goals for incident response help determine the structure of its incident response capability.

Control Enhancements: None.

References: NIST Special Publication 800-61.

Priority and Baseline Allocation:

P1	**LOW** IR-8	**MOD** IR-8	**HIGH** IR-8

FAMILY: MAINTENANCE **CLASS:** OPERATIONAL

MA-1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system maintenance family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The information system maintenance policy can be included as part of the general information security policy for the organization. System maintenance procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system maintenance policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** MA-1	**MOD** MA-1	**HIGH** MA-1

MA-2 CONTROLLED MAINTENANCE

Control: The organization:

a. Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;

b. Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;

c. Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;

d. Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and

e. Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.

Supplemental Guidance: The control is intended to address the information security aspects of the organization’s information system maintenance program. Related controls: MP-6, SI-2.

Control Enhancements:

(1) The organization maintains maintenance records for the information system that include:

(a) Date and time of maintenance;

(b) Name of the individual performing the maintenance;

(c) Name of escort, if necessary;

(d) A description of the maintenance performed; and

(e) A list of equipment removed or replaced (including identification numbers, if applicable).

(2) The organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs as required, producing up-to date, accurate, complete, and available records of all maintenance and repair actions, needed, in process, and completed.

References: None.

Priority and Baseline Allocation:

P2	**LOW** MA-2	**MOD** MA-2 (1)	**HIGH** MA-2 (1) (2)

MA-3 MAINTENANCE TOOLS

Control: The organization approves, controls, monitors the use of, and maintains on an ongoing basis, information system maintenance tools.

Supplemental Guidance: The intent of this control is to address the security-related issues arising from the hardware and software brought into the information system specifically for diagnostic and repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control. Related control: MP-6.

Control Enhancements:

(1) The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications.

Enhancement Supplemental Guidance: Maintenance tools include, for example, diagnostic and test equipment used to conduct maintenance on the information system.

(2) The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the information system.

(3) The organization prevents the unauthorized removal of maintenance equipment by one of the following: (i) verifying that there is no organizational information contained on the equipment; (ii) sanitizing or destroying the equipment; (iii) retaining the equipment within the facility; or (iv) obtaining an exemption from a designated organization official explicitly authorizing removal of the equipment from the facility.

(4) The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.

References: NIST Special Publication 800-88.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** MA-3 (1) (2)	**HIGH** MA-3 (1) (2) (3)

MA-4 NON-LOCAL MAINTENANCE

Control: The organization:

a. Authorizes, monitors, and controls non-local maintenance and diagnostic activities;

b. Allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the information system;

c. Employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions;

d. Maintains records for non-local maintenance and diagnostic activities; and

e. Terminates all sessions and network connections when non-local maintenance is completed.

Supplemental Guidance: Non-local maintenance and diagnostic activities are those activities conducted by individuals communicating through a network; either an external network (e.g., the Internet) or an internal network. Local maintenance and diagnostic activities are those activities carried out by individuals physically present at the information system or information system component and not communicating across a network connection. Identification and authentication techniques used in the establishment of non-local maintenance and diagnostic sessions are consistent with the network access requirements in IA-2. Strong authenticators include, for example, PKI where certificates are stored on a token protected by a password, passphrase, or biometric. Enforcing requirements in MA-4 is accomplished in part, by other controls. Related controls: AC-2, AC-3, AC-6, AC-17, AU-2, AU-3, IA-2, IA-8, MA-5, MP-6, SC-7.

Control Enhancements:

(1) The organization audits non-local maintenance and diagnostic sessions and designated organizational personnel review the maintenance records of the sessions.

(2) The organization documents, in the security plan for the information system, the installation and use of non-local maintenance and diagnostic connections.

(3) The organization:

(a) Requires that non-local maintenance and diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the system being serviced; or

(b) Removes the component to be serviced from the information system and prior to non-local maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities, and after the service is performed, inspects and sanitizes the component (with regard to potentially malicious software and surreptitious implants) before reconnecting the component to the information system.

(4) The organization protects non-local maintenance sessions through the use of a strong authenticator tightly bound to the user and by separating the maintenance session from other network sessions with the information system by either:

(a) Physically separated communications paths; or

(b) Logically separated communications paths based upon encryption.

Enhancement Supplemental Guidance: Related control: SC-13.

(5) The organization requires that:

(a) Maintenance personnel notify [*Assignment: organization-defined personnel*] when non-local maintenance is planned (i.e., date/time); and

(b) A designated organizational official with specific information security/information system knowledge approves the non-local maintenance.

(6) The organization employs cryptographic mechanisms to protect the integrity and confidentiality of non-local maintenance and diagnostic communications.

(7) The organization employs remote disconnect verification at the termination of non-local maintenance and diagnostic sessions.

References: FIPS Publications 140-2, 197, 201; NIST Special Publications 800-63, 800-88; CNSS Policy 15.

Priority and Baseline Allocation:

P1	**LOW** MA-4	**MOD** MA-4 (1) (2)	**HIGH** MA-4 (1) (2) (3)

MA-5 MAINTENANCE PERSONNEL

Control: The organization:

a. Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and

b. Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.

Supplemental Guidance: Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period. Related controls: IA-8, MA-5.

Control Enhancements:

(1) The organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

(a) Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified;

(b) Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

(c) In the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced.

Enhancement Supplemental Guidance: The intent of this control enhancement is to deny individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on the information system. Procedures for the use of maintenance personnel can be documented in the security plan for the information system.

(2) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are cleared (i.e., possess appropriate security clearances) for the highest level of information on the system.

(3) The organization ensures that personnel performing maintenance and diagnostic activities on an information system processing, storing, or transmitting classified information are U.S. citizens.

(4) The organization ensures that:

(a) Cleared foreign nationals (i.e., foreign nationals with appropriate security clearances), are used to conduct maintenance and diagnostic activities on an information system only when the system is jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

(b) Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on an information system are fully documented within a Memorandum of Agreement.

References: None.

Priority and Baseline Allocation:

P1	**LOW** MA-5	**MOD** MA-5	**HIGH** MA-5

MA-6 TIMELY MAINTENANCE

Control: The organization obtains maintenance support and/or spare parts for [*Assignment: organization-defined list of security-critical information system components and/or key information technology components*] within [*Assignment: organization-defined time period*] of failure.

Supplemental Guidance: The organization specifies those information system components that, when not operational, result in increased risk to organizations, individuals, or the Nation because the security functionality intended by that component is not being provided. Security-critical components include, for example, firewalls, guards, gateways, intrusion detection systems, audit repositories, authentication servers, and intrusion prevention systems. Related control: CP-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MA-6	**HIGH** MA-6

FAMILY: MEDIA PROTECTION **CLASS:** OPERATIONAL

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** MP-1	**MOD** MP-1	**HIGH** MP-1

MP-2 MEDIA ACCESS

Control: The organization restricts access to [*Assignment: organization-defined types of digital and non-digital media*] to [*Assignment: organization-defined list of authorized individuals*] using [*Assignment: organization-defined security measures*].

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Related controls: MP-4, PE-3.

Control Enhancements:

(1) **The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.**

Enhancement Supplemental Guidance: This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices).

(2) The information system uses cryptographic mechanisms to protect and restrict access to information on portable digital media.

References: FIPS Publication 199; NIST Special Publication 800-111.

Priority and Baseline Allocation:

P1	**LOW** MP-2	**MOD** MP-2 (1)	**HIGH** MP-2 (1)

MP-3 MEDIA MARKING

Control: The organization:

a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempts [*Assignment: organization-defined list of removable media types*] from marking as long as the exempted items remain within [*Assignment: organization-defined controlled areas*].

Supplemental Guidance: The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Some organizations, however, may require markings for public information indicating that the information is publicly releasable. Organizations may extend the scope of this control to include information system output devices containing organizational information, including, for example, monitors and printers. Marking of removable media and information system output is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-3	**HIGH** MP-3

MP-4 MEDIA STORAGE

Control: The organization:

a. Physically controls and securely stores [*Assignment: organization-defined types of digital and non-digital media*] within [*Assignment: organization-defined controlled areas*] using [*Assignment: organization-defined security measures*];

b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting the information and/or information system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.

As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information. Related controls: AC-3, AC-19, CP-6, CP-9, MP-2, PE-3.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to protect information in storage.

Enhancement Supplemental Guidance: Related control: SC-13.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-4	**HIGH** MP-4

MP-5 MEDIA TRANSPORT

Control: The organization:

a. Protects and controls [*Assignment: organization-defined types of digital and non-digital media*] during transport outside of controlled areas using [*Assignment: organization-defined security measures*];

b. Maintains accountability for information system media during transport outside of controlled areas; and

c. Restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.

Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Related controls: AC-19, CP-9.

Control Enhancements:

(1) [Withdrawn: Incorporated into MP-5].

(2) **The organization documents activities associated with the transport of information system media.**

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.

(3) **The organization employs an identified custodian throughout the transport of information system media.**

Enhancement Supplemental Guidance: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

(4) **The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.**

Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones). Related control: MP-4. Related controls: MP-2; SC-13.

References: FIPS Publication 199; NIST Special Publication 800-60.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** MP-5 (2) (4)	**HIGH** MP-5 (2) (3) (4)

MP-6 MEDIA SANITIZATION

Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.

Supplemental Guidance: This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or released for disposal. The organization employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information. The organization uses its discretion on the employment of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposal.

Control Enhancements:

(1) The organization tracks, documents, and verifies media sanitization and disposal actions.

(2) The organization tests sanitization equipment and procedures to verify correct performance [*Assignment: organization-defined frequency*].

(3) The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [*Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices*].

Enhancement Supplemental Guidance: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code to include code capable of initiating zero-day attacks. Organizations consider sanitization of portable, removable storage devices, for example, when such devices are first purchased from the manufacturer or vendor prior to initial use or when the organization loses a positive chain of custody for the device. An organizational assessment of risk guides the specific circumstances for employing the sanitization process. Related control: SI-3.

(4) The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.

(5) The organization sanitizes information system media containing classified information in accordance with NSA standards and policies.

(6) The organization destroys information system media that cannot be sanitized.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web: WWW.NSA.GOV/IA/GUIDANCE/MEDIA_DESTRUCTION_GUIDANCE/INDEX.SHTML.

Priority and Baseline Allocation:

P1	**LOW** MP-6	**MOD** MP-6	**HIGH** MP-6 (1) (2) (3)

FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION **CLASS:** OPERATIONAL

PE-1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the physical and environmental protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the physical and environmental protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PE-1	**MOD** PE-1	**HIGH** PE-1

PE-2 PHYSICAL ACCESS AUTHORIZATIONS

Control: The organization:

a. Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);

b. Issues authorization credentials;

c. Reviews and approves the access list and authorization credentials [*Assignment: organization-defined frequency*], removing from the access list personnel no longer requiring access.

Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. Related control: PE-3, PE-4.

Control Enhancements:

(1) The organization authorizes physical access to the facility where the information system resides based on position or role.

(2) The organization requires two forms of identification to gain access to the facility where the information system resides.

Enhancement Supplemental Guidance: Examples of forms of identification are identification badge, key card, cipher PIN, and biometrics.

(3) The organization restricts physical access to the facility containing an information system that processes classified information to authorized personnel with appropriate clearances and access authorizations.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-2	**MOD** PE-2	**HIGH** PE-2

PE-3 PHYSICAL ACCESS CONTROL

Control: The organization:

a. Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);

b. Verifies individual access authorizations before granting access to the facility;

c. Controls entry to the facility containing the information system using physical access devices and/or guards;

d. Controls access to areas officially designated as publicly accessible in accordance with the organization’s assessment of risk;

e. Secures keys, combinations, and other physical access devices;

f. Inventories physical access devices [*Assignment: organization-defined frequency*]; and

g. Changes combinations and keys [*Assignment: organization-defined frequency*] and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Supplemental Guidance: The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. Related controls: MP-2, MP-4, PE-2.

Control Enhancements:

(1) The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.

Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components. Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. See also PS-3, security requirements for personnel access to SCI.

(2) The organization performs security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or information system components.

Enhancement Supplemental Guidance: The extent/frequency or randomness of the checks is as deemed necessary by the organization to adequately mitigate risk associated with exfiltration.

(3) The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.

(4) The organization uses lockable physical casings to protect [*Assignment: organization-defined information system components*] from unauthorized physical access.

(5) The information system detects/prevents physical tampering or alteration of hardware components within the system.

(6) The organization employs a penetration testing process that includes [*Assignment: organization-defined frequency*], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

Enhancement Supplemental Guidance: Related control: CA-2.

References: FIPS Publication 201; NIST Special Publications 800-73, 800-76, 800-78; ICD 704; DCID 6/9.

Priority and Baseline Allocation:

P1	**LOW** PE-3	**MOD** PE-3	**HIGH** PE-3 (1)

PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM

Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.

Supplemental Guidance: Physical protections applied to information system distribution and transmission lines help prevent accidental damage, disruption, and physical tampering. Additionally, physical protections are necessary to help prevent eavesdropping or in transit modification of unencrypted transmissions. Protective measures to control physical access to information system distribution and transmission lines include: (i) locked wiring closets; (ii) disconnected or locked spare jacks; and/or (iii) protection of cabling by conduit or cable trays. Related control: PE-2.

Control Enhancements: None.

References: NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-4	**HIGH** PE-4

PE-5 ACCESS CONTROL FOR OUTPUT DEVICES

Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Supplemental Guidance: Monitors, printers, and audio devices are examples of information system output devices.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-5	**HIGH** PE-5

PE-6 MONITORING PHYSICAL ACCESS

Control: The organization:

a. Monitors physical access to the information system to detect and respond to physical security incidents;

b. Reviews physical access logs [*Assignment: organization-defined frequency*]; and

c. Coordinates results of reviews and investigations with the organization's incident response capability.

Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.

Control Enhancements:

(1) The organization monitors real-time physical intrusion alarms and surveillance equipment.

(2) The organization employs automated mechanisms to recognize potential intrusions and initiate designated response actions.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-6	**MOD** PE-6 (1)	**HIGH** PE-6 (1) (2)

PE-7 VISITOR CONTROL

Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.

Supplemental Guidance: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.

Control Enhancements:

(1) The organization escorts visitors and monitors visitor activity, when required.

(2) The organization requires two forms of identification for visitor access to the facility.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-7	**MOD** PE-7 (1)	**HIGH** PE-7 (1)

PE-8 ACCESS RECORDS

Control: The organization:

a. Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and

b. Reviews visitor access records [*Assignment: organization-defined frequency*].

Supplemental Guidance: Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.

Control Enhancements:

(1) The organization employs automated mechanisms to facilitate the maintenance and review of access records.

(2) The organization maintains a record of all physical access, both visitor and authorized individuals.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PE-8	**MOD** PE-8	**HIGH** PE-8 (1) (2)

PE-9 POWER EQUIPMENT AND POWER CABLING

Control: The organization protects power equipment and power cabling for the information system from damage and destruction.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs redundant and parallel power cabling paths.

(2) The organization employs automatic voltage controls for [*Assignment: organization-defined list of critical information system components*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-9	**HIGH** PE-9

PE-10 EMERGENCY SHUTOFF

Control: The organization:

a. Provides the capability of shutting off power to the information system or individual system components in emergency situations;

b. Places emergency shutoff switches or devices in [*Assignment: organization-defined location by information system or system component*] to facilitate safe and easy access for personnel; and

c. Protects emergency power shutoff capability from unauthorized activation.

Supplemental Guidance: This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.

Control Enhancements:

(1) [Withdrawn: Incorporated into PE-10].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-10	**HIGH** PE-10

PE-11 EMERGENCY POWER

Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization provides a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

(2) The organization provides a long-term alternate power supply for the information system that is self-contained and not reliant on external power generation.

Enhancement Supplemental Guidance: Long-term alternate power supplies for the information system are either manually or automatically activated.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-11	**HIGH** PE-11 (1)

PE-12 EMERGENCY LIGHTING

Control: The organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization provides emergency lighting for all areas within the facility supporting essential missions and business functions.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-12	**MOD** PE-12	**HIGH** PE-12

PE-13 FIRE PROTECTION

Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs fire detection devices/systems for the information system that activate automatically and notify the organization and emergency responders in the event of a fire.

(2) The organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to the organization and emergency responders.

(3) The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis.

(4) The organization ensures that the facility undergoes [*Assignment: organization-defined frequency*] fire marshal inspections and promptly resolves identified deficiencies.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-13	**MOD** PE-13 (1) (2) (3)	**HIGH** PE-13 (1) (2) (3)

PE-14 TEMPERATURE AND HUMIDITY CONTROLS

Control: The organization:

a. Maintains temperature and humidity levels within the facility where the information system resides at [*Assignment: organization-defined acceptable levels*]; and

b. Monitors temperature and humidity levels [*Assignment: organization-defined frequency*].

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs automatic temperature and humidity controls in the facility to prevent fluctuations potentially harmful to the information system.

(2) The organization employs temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-14	**MOD** PE-14	**HIGH** PE-14

PE-15 WATER DAMAGE PROTECTION

Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.

Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) The organization employs mechanisms that, without the need for manual intervention, protect the information system from water damage in the event of a water leak.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-15	**MOD** PE-15	**HIGH** PE-15 (1)

PE-16 DELIVERY AND REMOVAL

Control: The organization authorizes, monitors, and controls [*Assignment: organization-defined types of information system components*] entering and exiting the facility and maintains records of those items.

Supplemental Guidance: Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** PE-16	**MOD** PE-16	**HIGH** PE-16

PE-17 ALTERNATE WORK SITE

Control: The organization:

a. Employs [*Assignment: organization-defined management, operational, and technical information system security controls*] at alternate work sites;

b. Assesses as feasible, the effectiveness of security controls at alternate work sites; and

c. Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

Supplemental Guidance: Alternate work sites may include, for example, government facilities or private residences of employees. The organization may define different sets of security controls for specific alternate work sites or types of sites.

Control Enhancements: None.

References: NIST Special Publication 800-46.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** PE-17	**HIGH** PE-17

PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS

Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.

Control Enhancements:

(1) **The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.**

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** PE-18	**HIGH** PE-18 (1)

PE-19 INFORMATION LEAKAGE

Control: The organization protects the information system from information leakage due to electromagnetic signals emanations.

Supplemental Guidance: The security categorization of the information system (with respect to confidentiality) and organizational security policy guides the application of safeguards and countermeasures employed to protect the information system against information leakage due to electromagnetic signals emanations.

Control Enhancements:

(1) **The organization ensures that information system components, associated data communications, and networks are protected in accordance with: (i) national emissions and TEMPEST policies and procedures; and (ii) the sensitivity of the information being transmitted.**

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: PLANNING **CLASS:** MANAGEMENT

PL-1 SECURITY PLANNING POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security planning family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The security planning policy addresses the overall policy requirements for confidentiality, integrity, and availability and can be included as part of the general information security policy for the organization. Security planning procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security planning policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-18, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PL-1	**MOD** PL-1	**HIGH** PL-1

PL-2 SYSTEM SECURITY PLAN

Control: The organization:

a. Develops a security plan for the information system that:

- Is consistent with the organization’s enterprise architecture;
- Explicitly defines the authorization boundary for the system;
- Describes the operational context of the information system in terms of missions and business processes;
- Provides the security category and impact level of the information system including supporting rationale;
- Describes the operational environment for the information system;
- Describes relationships with or connections to other information systems;
- Provides an overview of the security requirements for the system;
- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and
- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;

b. Reviews the security plan for the information system [*Assignment: organization-defined frequency*]; and

c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.

Supplemental Guidance: The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Related controls: PM-1, PM-7, PM-8, PM-9, PM-11.

Control Enhancements:

(1) The organization:

(a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and

(b) Reviews and updates the CONOPS [*Assignment: organization-defined frequency*].

Enhancement Supplemental Guidance: The security CONOPS may be included in the security plan for the information system.

(2) The organization develops a functional architecture for the information system that identifies and maintains:

(a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface;

(b) User roles and the access privileges assigned to each role;

(c) Unique security requirements;

(d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and

(e) Restoration priority of information or information system services.

Enhancement Supplemental Guidance: Unique security requirements for the information system include, for example, encryption of key data elements at rest. Specific protection needs for the information system include, for example, the Privacy Act and Health Insurance Portability and Accountability Act.

References: NIST Special Publication 800-18.

Priority and Baseline Allocation:

P1	**LOW** PL-2	**MOD** PL-2	**HIGH** PL-2

PL-3 SYSTEM SECURITY PLAN UPDATE

[Withdrawn: Incorporated into PL-2].

PL-4 RULES OF BEHAVIOR

Control: The organization:

a. Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and

b. Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.

Supplemental Guidance: The organization considers different sets of rules based on user roles and responsibilities, for example, differentiating between the rules that apply to privileged users and rules that apply to general users. Electronic signatures are acceptable for use in acknowledging rules of behavior. Related control: PS-6.

Control Enhancements:

(1) The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.

References: NIST Publication 800-18.

Priority and Baseline Allocation:

P1	**LOW** PL-4	**MOD** PL-4	**HIGH** PL-4

PL-5 PRIVACY IMPACT ASSESSMENT

Control: The organization conducts a privacy impact assessment on the information system in accordance with OMB policy.

Supplemental Guidance: None.

Control Enhancements: None.

References: OMB Memorandum 03-22.

Priority and Baseline Allocation:

P1	**LOW** PL-5	**MOD** PL-5	**HIGH** PL-5

PL-6 SECURITY-RELATED ACTIVITY PLANNING

Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

Supplemental Guidance: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or nonurgent unplanned) situations.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** Not Selected	**MOD** PL-6	**HIGH** PL-6

FAMILY: PERSONNEL SECURITY **CLASS:** OPERATIONAL

PS-1 PERSONNEL SECURITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the personnel security family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the personnel security policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** PS-1	**MOD** PS-1	**HIGH** PS-1

PS-2 POSITION CATEGORIZATION

Control: The organization:

a. Assigns a risk designation to all positions;

b. Establishes screening criteria for individuals filling those positions; and

c. Reviews and revises position risk designations [*Assignment: organization-defined frequency*].

Supplemental Guidance: Position risk designations are consistent with Office of Personnel Management policy and guidance. The screening criteria include explicit information security role appointment requirements (e.g., training, security clearance).

Control Enhancements: None.

References: 5 CFR 731.106(a).

Priority and Baseline Allocation:

P1	**LOW** PS-2	**MOD** PS-2	**HIGH** PS-2

PS-3 PERSONNEL SCREENING

Control: The organization:

a. Screens individuals prior to authorizing access to the information system; and

b. Rescreens individuals according to [*Assignment: organization-defined list of conditions requiring rescreening and, where re-screening is so indicated, the frequency of such rescreening*].

Supplemental Guidance: Screening and rescreening are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidance, and the criteria established for the risk designation of the assigned position. The organization may define different rescreening conditions and frequencies for personnel accessing the information system based on the type of information processed, stored, or transmitted by the system.

Control Enhancements:

(1) The organization ensures that every user accessing an information system processing, storing, or transmitting classified information is cleared and indoctrinated to the highest classification level of the information on the system.

(2) The organization ensures that every user accessing an information system processing, storing, or transmitting types of classified information which require formal indoctrination, is formally indoctrinated for all of the relevant types of information on the system.

Enhancement Supplemental Guidance: Types of information requiring formal indoctrination include, for example, Special Access Program (SAP), Restricted Data (RD), and Sensitive Compartment Information (SCI).

References: 5 CFR 731.106; FIPS Publications 199, 201; NIST Special Publications 800-73, 800-76, 800-78; ICD 704.

Priority and Baseline Allocation:

P1	**LOW** PS-3	**MOD** PS-3	**HIGH** PS-3

PS-4 PERSONNEL TERMINATION

Control: The organization, upon termination of individual employment:

a. Terminates information system access;

b. Conducts exit interviews;

c. Retrieves all security-related organizational information system-related property; and

d. Retains access to organizational information and information systems formerly controlled by terminated individual.

Supplemental Guidance: Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that individuals understand any security constraints imposed by being former employees and that proper accountability is achieved for all information system-related property. Exit interviews may not be possible for some employees (e.g., in the case of job abandonment, some illnesses, and nonavailability of supervisors). Exit interviews are important for individuals with security clearances. Timely execution of this control is particularly essential for employees or contractors terminated for cause.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PS-4	**MOD** PS-4	**HIGH** PS-4

PS-5 PERSONNEL TRANSFER

Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates [*Assignment: organization-defined transfer or reassignment actions*] within [*Assignment: organization-defined time period following the formal transfer action*].

Supplemental Guidance: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** PS-5	**MOD** PS-5	**HIGH** PS-5

PS-6 ACCESS AGREEMENTS

Control: The organization:

a. Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and

b. Reviews/updates the access agreements [*Assignment: organization-defined frequency*].

Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. Related control: PL-4.

Control Enhancements:

(1) The organization ensures that access to information with special protection measures is granted only to individuals who:

(a) Have a valid access authorization that is demonstrated by assigned official government duties; and

(b) Satisfy associated personnel security criteria.

Enhancement Supplemental Guidance: Information with special protection measures includes, for example, privacy information, proprietary information, and Sources and Methods Information (SAMI). Personnel security criteria include, for example, position sensitivity background screening requirements.

(2) The organization ensures that access to classified information with special protection measures is granted only to individuals who:

(a) Have a valid access authorization that is demonstrated by assigned official government duties;

(b) Satisfy associated personnel security criteria consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and

(c) Have read, understand, and signed a nondisclosure agreement.

Enhancement Supplemental Guidance: Examples of special protection measures include, for example, collateral, Special Access Program (SAP) and Sensitive Compartmented Information (SCI).

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-6	**MOD** PS-6	**HIGH** PS-6

PS-7 THIRD-PARTY PERSONNEL SECURITY

Control: The organization:

a. Establishes personnel security requirements including security roles and responsibilities for third-party providers;

b. Documents personnel security requirements; and

c. Monitors provider compliance.

Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents.

Control Enhancements: None.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** PS-7	**MOD** PS-7	**HIGH** PS-7

PS-8 PERSONNEL SANCTIONS

Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.

Supplemental Guidance: The sanctions process is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The process is described in access agreements and can be included as part of the general personnel policies and procedures for the organization. Related controls: PL-4, PS-6.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P3	**LOW** PS-8	**MOD** PS-8	**HIGH** PS-8

FAMILY: RISK ASSESSMENT **CLASS:** MANAGEMENT

RA-1 RISK ASSESSMENT POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the risk assessment family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The risk assessment policy can be included as part of the general information security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the risk assessment policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-30,800-100.

Priority and Baseline Allocation:

P1	**LOW** RA-1	**MOD** RA-1	**HIGH** RA-1

RA-2 SECURITY CATEGORIZATION

Control: The organization:

a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and

c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.

Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be comprised through a loss of confidentiality, integrity, or availability. The organization conducts the security categorization process as an organization-wide activity with the involvement of the chief information officer, senior information security officer, information system owner, mission owners, and information owners/stewards. The organization also considers potential adverse impacts to other organizations and, in accordance with the USA PATRIOT Act of 2001 and Homeland Security Presidential Directives, potential national-level adverse impacts in categorizing the information system. The security categorization process facilitates the creation of an *inventory* of information assets, and in conjunction with CM-8, a mapping to the information system components where the information is processed, stored, and transmitted. Related controls: CM-8, MP-4, SC-7.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-60.

Priority and Baseline Allocation:

P1	**LOW** RA-2	**MOD** RA-2	**HIGH** RA-2

RA-3 RISK ASSESSMENT

Control: The organization:

a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;

b. Documents risk assessment results in [*Selection: security plan; risk assessment report;* [*Assignment: organization-defined document*]];

c. Reviews risk assessment results [*Assignment: organization-defined frequency*]; and

d. Updates the risk assessment [*Assignment: organization-defined frequency*] or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.

Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Nation based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. The General Services Administration provides tools supporting that portion of the risk assessment dealing with public access to federal information systems.

Risk assessments (either formal or informal) can be conducted by organizations at various steps in the Risk Management Framework including: information system categorization; security control selection; security control implementation; security control assessment; information system authorization; and security control monitoring. RA-3 is a noteworthy security control in that the control must be partially *implemented* prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in the security control selection process during the application of tailoring guidance for security control baselines and when considering supplementing the tailored baselines with additional security controls or control enhancements.

Control Enhancements: None.

References: NIST Special Publication 800-30.

Priority and Baseline Allocation:

P1	**LOW** RA-3	**MOD** RA-3	**HIGH** RA-3

RA-4 RISK ASSESSMENT UPDATE

[Withdrawn: Incorporated into RA-3].

RA-5 VULNERABILITY SCANNING

Control: The organization:

a. Scans for vulnerabilities in the information system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system/applications are identified and reported;

b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:

- Enumerating platforms, software flaws, and improper configurations;
- Formatting and making transparent, checklists and test procedures; and
- Measuring vulnerability impact;

c. Analyzes vulnerability scan reports and results from security control assessments;

d. Remediates legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk; and

e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).

Supplemental Guidance: The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. The Common Weakness Enumeration (CWE) and the National Vulnerability Database (NVD) are also excellent sources for vulnerability information. In addition, security control assessments such as red team exercises are another source of potential vulnerabilities for which to scan. Related controls: CA-2, CM-6, RA-3, SI-2.

Control Enhancements:

(1) The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.

(2) The organization updates the list of information system vulnerabilities scanned [*Assignment: organization-defined frequency*] or when new vulnerabilities are identified and reported.

(3) The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).

(4) The organization attempts to discern what information about the information system is discoverable by adversaries.

(5) The organization includes privileged access authorization to [*Assignment: organization-identified information system components*] for selected vulnerability scanning activities to facilitate more thorough scanning.

(6) The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in information system vulnerabilities.

(7) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials.

(8) The organization reviews historic audit logs to determine if a vulnerability identified in the information system has been previously exploited.

(9) The organization employs an independent penetration agent or penetration team to:

(a) Conduct a vulnerability analysis on the information system; and

(b) Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.

Enhancement Supplemental Guidance: A standard method for penetration testing includes: (i) pre-test analysis based on full knowledge of the target information system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario.

References: NIST Special Publications 800-40, 800-70, 800-115; Web: CWE.MITRE.ORG; NVD.NIST.GOV.

Priority and Baseline Allocation:

P1	**LOW** RA-5	**MOD** RA-5 (1)	**HIGH** RA-5 (1) (2) (3) (4) (5) (7)

FAMILY: SYSTEM AND SERVICES ACQUISITION **CLASS:** MANAGEMENT

SA-1 SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and services acquisition family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and services acquisition policy can be included as part of the general information security policy for the organization. System and services acquisition procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and services acquisition policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SA-1	**MOD** SA-1	**HIGH** SA-1

SA-2 ALLOCATION OF RESOURCES

Control: The organization:

a. Includes a determination of information security requirements for the information system in mission/business process planning;

b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and

c. Establishes a discrete line item for information security in organizational programming and budgeting documentation.

Supplemental Guidance: Related controls: PM-3, PM-11.

Control Enhancements: None.

References: NIST Special Publication 800-65.

Priority and Baseline Allocation:

P1	**LOW** SA-2	**MOD** SA-2	**HIGH** SA-2

SA-3 LIFE CYCLE SUPPORT

Control: The organization:

a. Manages the information system using a system development life cycle methodology that includes information security considerations;

b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and

c. Identifies individuals having information system security roles and responsibilities.

Supplemental Guidance: Related control: PM-7.

Control Enhancements: None.

References: NIST Special Publication 800-64.

Priority and Baseline Allocation:

P1	**LOW** SA-3	**MOD** SA-3	**HIGH** SA-3

SA-4 ACQUISITIONS

Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards:

a. Security functional requirements/specifications;

b. Security-related documentation requirements; and

c. Developmental and evaluation-related assurance requirements.

Supplemental Guidance: The acquisition documents for information systems, information system components, and information system services include, either explicitly or by reference, security requirements that describe: (i) required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements); (ii) required design and development processes; (iii) required test and evaluation procedures; and (iv) required documentation. The requirements in the acquisition documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented. Acquisition documents also include requirements for appropriate information system documentation. The documentation addresses user and system administrator guidance and information regarding the implementation of the security controls in the information system. The level of detail required in the documentation is based on the security categorization for the information system. In addition, the required documentation includes security configuration settings and security implementation guidance. FISMA reporting instructions provide guidance on configuration requirements for federal information systems.

Control Enhancements:

(1) The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.

(2) The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.

(3) The organization requires software vendors/manufacturers to demonstrate that their software development processes employ state-of-the-practice software and security engineering methods, quality control processes, and validation techniques to minimize flawed or malformed software.

(4) The organization ensures that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

(5) The organization requires in acquisition documents, that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.

(6) The organization:

(a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that composes an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and

(b) Ensures that these products have been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures.

Enhancement Supplemental Guidance: COTS IA or IA-enabled information technology products used to protect classified information by cryptographic means, may be required to use NSA-approved key management.

(7) The organization:

(a) Limits the use of commercially provided information technology products to those products that have been successfully evaluated against a validated U.S. Government Protection Profile for a specific technology type, if such a profile exists; and

(b) Requires, if no U.S. Government Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, then the cryptographic module is FIPS-validated.

References: ISO/IEC 15408; FIPS 140-2; NIST Special Publications 800-23, 800-35, 800-36, 800-64, 800-70; Web: WWW.NIAP-CCEVS.ORG.

Priority and Baseline Allocation:

P1	**LOW** SA-4	**MOD** SA-4 (1) (4)	**HIGH** SA-4 (1) (2) (4)

SA-5 INFORMATION SYSTEM DOCUMENTATION

Control: The organization:

a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:

- Secure configuration, installation, and operation of the information system;
- Effective use and maintenance of security features/functions; and
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and

b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:

- User-accessible security features/functions and how to effectively use those security features/functions;
- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and
- User responsibilities in maintaining the security of the information and information system; and

c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.

Supplemental Guidance: The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

Control Enhancements:

(1) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.

(2) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.

(3) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.

(4) The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the low-level design of the information system in terms of modules and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.

Enhancement Supplemental Guidance: Each subsystem within an information system can contain one or more modules.

(5) The organization obtains, protects as required, and makes available to authorized personnel, the source code for the information system to permit analysis and testing.

References: None.

Priority and Baseline Allocation:

P2	**LOW** SA-5	**MOD** SA-5 (1) (3)	**HIGH** SA-5 (1) (2) (3)

SA-6 SOFTWARE USAGE RESTRICTIONS

Control: The organization:

a. Uses software and associated documentation in accordance with contract agreements and copyright laws;

b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and

c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.

Control Enhancements:

(1) The organization:

(a) Prohibits the use of binary or machine executable code from sources with limited or no warranty without accompanying source code; and

(b) Provides exceptions to the source code requirement only for compelling mission/operational requirements when no alternative solutions are available and with the express written consent of the authorizing official.

Enhancement Supplemental Guidance: Software products without accompanying source code from sources with limited or no warranty are assessed for potential security impacts. The assessment addresses the fact that these types of software products are difficult or impossible to review, repair, or extend, given that the organization does not have access to the original source code and there is no owner who could make such repairs on behalf of the organization.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SA-6	**MOD** SA-6	**HIGH** SA-6

SA-7 USER-INSTALLED SOFTWARE

Control: The organization enforces explicit rules governing the installation of software by users.

Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SA-7	**MOD** SA-7	**HIGH** SA-7

SA-8 SECURITY ENGINEERING PRINCIPLES

Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.

Supplemental Guidance: The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.

Control Enhancements: None.

References: NIST Special Publication 800-27.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-8	**HIGH** SA-8

SA-9 EXTERNAL INFORMATION SYSTEM SERVICES

Control: The organization:

a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance;

b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and

c. Monitors security control compliance by external service providers.

Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.

Control Enhancements:

(1) The organization:

(a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and

(b) Ensures that the acquisition or outsourcing of dedicated information security services is approved by [*Assignment: organization-defined senior organizational official*].

Enhancement Supplemental Guidance: Dedicated information security services include, for example, incident monitoring, analysis and response, operation of information security-related devices such as firewalls, or key management services.

References: NIST Special Publication 800-35.

Priority and Baseline Allocation:

P1	**LOW** SA-9	**MOD** SA-9	**HIGH** SA-9

SA-10 DEVELOPER CONFIGURATION MANAGEMENT

Control: The organization requires that information system developers/integrators:

a. Perform configuration management during information system design, development, implementation, and operation;

b. Manage and control changes to the information system;

c. Implement only organization-approved changes;

d. Document approved changes to the information system; and

e. Track security flaws and flaw resolution.

Supplemental Guidance: Related controls: CM-3, CM-4, CM-9.

Control Enhancements:

(1) The organization requires that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery.

(2) The organization provides an alternative configuration management process with organizational personnel in the absence of dedicated developer/integrator configuration management team.

Enhancement Supplemental Guidance: The configuration management process includes key organizational personnel that are responsible for reviewing and approving proposed changes to the information system, and security personnel that conduct impact analyses prior to the implementation of any changes to the system.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SA-10	**HIGH** SA-10

SA-11 DEVELOPER SECURITY TESTING

Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):

a. Create and implement a security test and evaluation plan;

b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and

c. Document the results of the security testing/evaluation and flaw remediation processes.

Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.

Control Enhancements:

(1) The organization requires that information system developers/integrators employ code analysis tools to examine software for common flaws and document the results of the analysis.

(2) The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.

(3) The organization requires that information system developers/integrators create a security test and evaluation plan and implement the plan under the witness of an independent verification and validation agent.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SA-11	**HIGH** SA-11

SA-12 SUPPLY CHAIN PROTECTION

Control: The organization protects against supply chain threats by employing: [*Assignment: organization-defined list of measures to protect against supply chain threats*] as part of a comprehensive, defense-in-breadth information security strategy.

Supplemental Guidance: A defense-in-breadth approach helps to protect information systems (including the information technology products that compose those systems) throughout the system development life cycle (i.e., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). This is accomplished by the identification, management, and elimination of vulnerabilities at each phase of the life cycle and the use of complementary, mutually reinforcing strategies to mitigate risk.

Control Enhancements:

(1) **The organization purchases all anticipated information system components and spares in the initial acquisition.**

Enhancement Supplemental Guidance: Stockpiling information system components and spares avoids the need to use less trustworthy secondary or resale markets in future years.

(2) **The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.**

Enhancement Supplemental Guidance: The organization reviews supplier claims with regard to the use of appropriate security processes in the development and manufacture of information system components or products.

(3) **The organization uses trusted shipping and warehousing for information systems, information system components, and information technology products.**

Enhancement Supplemental Guidance: Trusted shipping and warehousing reduces opportunities for subversive activities or interception during transit. Examples of supporting techniques include the use of a geographically aware beacon to detect shipment diversions or delays. Related control: PE-16.

(4) **The organization employs a diverse set of suppliers for information systems, information system components, information technology products, and information system services.**

Enhancement Supplemental Guidance: Diversification of suppliers is intended to limit the potential harm from a given supplier in a supply chain, increasing the work factor for an adversary.

(5) **The organization employs standard configurations for information systems, information system components, and information technology products.**

Enhancement Supplemental Guidance: By avoiding the purchase of custom configurations for information systems, information system components, and information technology products, the organization limits the possibility of acquiring systems and products that have been corrupted via the supply chain actions targeted at the organization.

(6) **The organization minimizes the time between purchase decisions and delivery of information systems, information system components, and information technology products.**

Enhancement Supplemental Guidance: By minimizing the time between purchase decisions and required delivery of information systems, information system components, and information technology products, the organization limits the opportunity for an adversary to corrupt the purchased system, component, or product.

(7) **The organization employs independent analysis and penetration testing against delivered information systems, information system components, and information technology products.**

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-12

SA-13 TRUSTWORTHINESS

Control: The organization requires that the information system meets [*Assignment: organization-defined level of trustworthiness*].

Supplemental Guidance: The intent of this control is to ensure that organizations recognize the importance of trustworthiness and making explicit trustworthiness decisions when designing, developing, and implementing organizational information systems. Trustworthiness is a characteristic or property of an information system that expresses the degree to which the system can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system. Trustworthy information systems are systems that are capable of being trusted to operate within defined levels of *risk* despite the environmental disruptions, human errors, and purposeful attacks that are expected to occur in the specified environments of operation. Two factors affecting the trustworthiness of an information system include: (i) *security functionality* (i.e., the security features or functions employed within the system); and (ii) *security assurance* (i.e., the grounds for confidence that the security functionality is effective in its application).

Appropriate security functionality for the information system can be obtained by using the Risk Management Framework (Steps 1, 2, and 3) to select and implement the necessary management, operational, and technical security controls necessary to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. Appropriate security assurance can be obtained by: (i) the actions taken by developers and implementers of security controls with regard to the design, development, implementation, and operation of those controls; and (ii) the actions taken by assessors to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Developers and implementers can increase the assurance in security controls by employing well-defined security policy models, structured, disciplined, and rigorous hardware and software development techniques, and sound system/security engineering principles. Assurance is also based on the assessment of evidence produced during the initiation, acquisition/development, implementation, and operations/maintenance phases of the system development life cycle. For example, developmental evidence may include the techniques and methods used to design and develop security functionality. Operational evidence may include flaw reporting and remediation, the results of security incident reporting, and the results of the ongoing monitoring of security controls. Independent assessments by qualified assessors may include analyses of the evidence as well as testing, inspections, and audits. Minimum assurance requirements are described in Appendix E.

Explicit trustworthiness decisions highlight situations where achieving the information system resilience and security capability necessary to withstand cyber attacks from adversaries with certain threat capabilities may require adjusting the risk management strategy, the design of mission/business processes with regard to automation, the selection and implementation rigor of management and operational protections, or the selection of information technology components with higher levels of trustworthiness. Trustworthiness may be defined on a component-by-component, subsystem-by-subsystem, or function-by-function basis. It is noted, however, that typically functions, subsystems, and components are highly interrelated, making separation by trustworthiness perhaps problematic and at a minimum, something that likely requires careful attention in order to achieve practically useful results. Related controls: RA-2, SA-4, SA-8, SC-3.

Control Enhancements: None.

References: FIPS Publications 199, 200; NIST Special Publications 800-53, 800-53A, 800-60, 800-64.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SA-13

SA-14 CRITICAL INFORMATION SYSTEM COMPONENTS

Control: The organization:

a. Determines [*Assignment: organization-defined list of critical information system components that require re-implementation*]; and

b. Re-implements or custom develops such information system components.

Supplemental Guidance: The underlying assumption is that the list of information technology products defined by the organization cannot be trusted due to threats from the supply chain that the organization finds unacceptable. The organization re-implements or custom develops such components to satisfy requirements for high assurance. Related controls: SA-12, SA-13.

Control Enhancements:

(1) The organization:

(a) Identifies information system components for which alternative sourcing is not viable; and

(b) Employs [*Assignment: organization-defined measures*] to ensure that critical security controls for the information system components are not compromised.

Enhancement Supplemental Guidance: Measures that the organization considers implementing include, for example, enhanced auditing, restrictions on source code and system utility access, and protection from deletion of system and application files.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND COMMUNICATIONS PROTECTION **CLASS:** TECHNICAL

SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and communications protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and communications protection policy can be included as part of the general information security policy for the organization. System and communications protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and communications protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SC-1	**MOD** SC-1	**HIGH** SC-1

SC-2 APPLICATION PARTITIONING

Control: The information system separates user functionality (including user interface services) from information system management functionality.

Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.

Control Enhancements:

(1) **The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users.**

Enhancement Supplemental Guidance: The intent of this control enhancement is to ensure that administration options are not available to general users (including prohibiting the use of the grey-out option commonly used to eliminate accessibility to such information). For example, administration options are not presented until the user has appropriately established a session with administrator privileges.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-2	**HIGH** SC-2

SC-3 SECURITY FUNCTION ISOLATION

Control: The information system isolates security functions from nonsecurity functions.

Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process. Related control: SA-13.

Control Enhancements:

(1) The information system implements underlying hardware separation mechanisms to facilitate security function isolation.

(2) The information system isolates security functions enforcing access and information flow control from both nonsecurity functions and from other security functions.

(3) The organization implements an information system isolation boundary to minimize the number of nonsecurity functions included within the boundary containing security functions.

Enhancement Supplemental Guidance: Nonsecurity functions contained within the isolation boundary are considered security-relevant.

(4) The organization implements security functions as largely independent modules that avoid unnecessary interactions between modules.

(5) The organization implements security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-3

SC-4 INFORMATION IN SHARED RESOURCES

Control: The information system prevents unauthorized and unintended information transfer via shared system resources.

Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.

Control Enhancements:

(1) The information system does not share resources that are used to interface with systems operating at different security levels.

Enhancement Supplemental Guidance: Shared resources include, for example, memory, input/output queues, and network interface cards.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-4	**HIGH** SC-4

SC-5 DENIAL OF SERVICE PROTECTION

Control: The information system protects against or limits the effects of the following types of denial of service attacks: [*Assignment: organization-defined list of types of denial of service attacks or reference to source for current list*].

Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.

Control Enhancements:

(1) **The information system restricts the ability of users to launch denial of service attacks against other information systems or networks.**

(2) **The information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.**

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-5	**MOD** SC-5	**HIGH** SC-5

SC-6 RESOURCE PRIORITY

Control: The information system limits the use of resources by priority.

Supplemental Guidance: Priority protection helps prevent a lower-priority process from delaying or interfering with the information system servicing any higher-priority process. This control does not apply to components in the information system for which there is only a single user/role.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-7 BOUNDARY PROTECTION

Control: The information system:

a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and

b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance: Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ).

The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.

Control Enhancements:

(1) The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.

Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.

(2) The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.

(3) The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.

Enhancement Supplemental Guidance: The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.

(4) The organization:

(a) Implements a managed interface for each external telecommunication service;

(b) Establishes a traffic flow policy for each managed interface;

(c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;

(d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;

(e) Reviews exceptions to the traffic flow policy [*Assignment: organization-defined frequency*]; and

(f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.

(5) The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).

(6) The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.

(7) The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.

Enhancement Supplemental Guidance: This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent *split-tunneling*. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.

(8) The information system routes [*Assignment: organization-defined internal communications traffic*] to [*Assignment: organization-defined external networks*] through authenticated proxy servers within the managed interfaces of boundary protection devices.

Enhancement Supplemental Guidance: External networks are networks outside the control of the organization. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Proxy servers are also configurable with organization-defined lists of authorized and unauthorized websites.

(9) The information system, at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.

Enhancement Supplemental Guidance: Detecting internal actions that may pose a security threat to external information systems is sometimes termed extrusion detection. Extrusion detection at the information system boundary includes the analysis of network traffic (incoming as well as outgoing) looking for indications of an internal threat to the security of external systems.

(10) The organization prevents the unauthorized exfiltration of information across managed interfaces.

Enhancement Supplemental Guidance: Measures to prevent unauthorized exfiltration of information from the information system include, for example: (i) strict adherence to protocol formats; (ii) monitoring for indications of beaconing from the information system; (iii) monitoring for use of steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect deviations from the volume or types of traffic expected within the organization. Examples of devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layer.

(11) The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.

(12) The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.

Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.

(13) The organization isolates [*Assignment: organization defined key information security tools, mechanisms, and support components*] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.

(14) The organization protects against unauthorized physical connections across the boundary protections implemented at [*Assignment: organization-defined list of managed interfaces*].

Enhancement Supplemental Guidance: Information systems operating at different security categories may routinely share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items. Related control: PE-4.

(15) The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.

Enhancement Supplemental Guidance: Related controls: AC-2, AC-3, AC-4, AU-2.

(16) The information system prevents discovery of specific system components (or devices) composing a managed interface.

Enhancement Supplemental Guidance: This control enhancement is intended to protect the network addresses of information system components that are part of the managed interface from discovery through common tools and techniques used to identify devices on a network. The network addresses are not available for discovery (e.g., not published or entered in the domain name system), requiring prior knowledge for access. Another obfuscation technique is to periodically change network addresses.

(17) The organization employs automated mechanisms to enforce strict adherence to protocol format.

Enhancement Supplemental Guidance: Automated mechanisms used to enforce protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification (e.g., IEEE) at the application layer and serve to identify significant vulnerabilities that cannot be detected by devices operating at the network or transport layer.

(18) The information system fails securely in the event of an operational failure of a boundary protection device.

Enhancement Supplemental Guidance: Fail secure is a condition achieved by the application of a set of information system mechanisms to ensure that in the event of an operational failure of a boundary protection device at a managed interface (e.g., router, firewall, guard, application gateway residing on a protected subnetwork commonly referred to as a demilitarized zone), the system does not enter into an unsecure state where intended security properties no longer hold. A failure of a boundary protection device cannot lead to, or cause information external to the boundary protection device to enter the device, nor can a failure permit unauthorized information release.

References: FIPS Publication 199; NIST Special Publications 800-41, 800-77.

Priority and Baseline Allocation:

P1	**LOW** SC-7	**MOD** SC-7 (1) (2) (3) (4) (5) (7)	**HIGH** SC-7 (1) (2) (3) (4) (5) (6) (7) (8)

SC-8 TRANSMISSION INTEGRITY

Control: The information system protects the integrity of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

(2) The information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.

Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously modified at data aggregation or protocol transformation points, compromising the integrity of the information.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-81, 800-113; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-8 (1)	**HIGH** SC-8 (1)

SC-9 TRANSMISSION CONFIDENTIALITY

Control: The information system protects the confidentiality of transmitted information.

Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.

Control Enhancements:

(1) The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by alternative physical measures.

Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.

(2) The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission.

Enhancement Supplemental Guidance: Information can be intentionally and/or maliciously disclosed at data aggregation or protocol transformation points, compromising the confidentiality of the information.

References: FIPS Publications 140-2, 197; NIST Special Publications 800-52, 800-77, 800-113; CNSS Policy 15; NSTISSI No. 7003.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-9 (1)	**HIGH** SC-9 (1)

SC-10 NETWORK DISCONNECT

Control: The information system terminates the network connection associated with a communications session at the end of the session or after [*Assignment: organization-defined time period*] of inactivity.

Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SC-10	**HIGH** SC-10

SC-11 TRUSTED PATH

Control: The information system establishes a trusted communications path between the user and the following security functions of the system: [*Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication*].

Supplemental Guidance: A trusted path is employed for high-confidence connections between the security functions of the information system and the user (e.g., for login).

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system.

Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.

Control Enhancements:

(1) **The organization maintains availability of information in the event of the loss of cryptographic keys by users.**

(2) **The organization produces, controls, and distributes symmetric cryptographic keys using [*Selection: NIST-approved, NSA-approved*] key management technology and processes.**

(3) **The organization produces, controls, and distributes symmetric and asymmetric cryptographic keys using NSA-approved key management technology and processes.**

(4) **The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 certificates or prepositioned keying material.**

(5) **The organization produces, controls, and distributes asymmetric cryptographic keys using approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key.**

References: NIST Special Publications 800-56, 800-57.

Priority and Baseline Allocation:

P1	**LOW** SC-12	**MOD** SC-12	**HIGH** SC-12 (1)

SC-13 USE OF CRYPTOGRAPHY

Control: The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Supplemental Guidance: None.

Control Enhancements:

(1) The organization employs, at a minimum, FIPS-validated cryptography to protect unclassified information.

(2) The organization employs NSA-approved cryptography to protect classified information.

(3) The organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals.

(4) The organization employs [*Selection: FIPS-validated; NSA-approved*] cryptography to implement digital signatures.

References: FIPS Publication 140-2; Web: CSRC.NIST.GOV/CRYPTVAL, WWW.CNSS.GOV.

Priority and Baseline Allocation:

P1	**LOW** SC-13	**MOD** SC-13	**HIGH** SC-13

SC-14 PUBLIC ACCESS PROTECTIONS

Control: The information system protects the integrity and availability of publicly available information and applications.

Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-14	**MOD** SC-14	**HIGH** SC-14

SC-15 COLLABORATIVE COMPUTING DEVICES

Control: The information system:

a. Prohibits remote activation of collaborative computing devices with the following exceptions: [*Assignment: organization-defined exceptions where remote activation is to be allowed*]; and

b. Provides an explicit indication of use to users physically present at the devices.

Supplemental Guidance: Collaborative computing devices include, for example, networked white boards, cameras, and microphones. Explicit indication of use includes, for example, signals to users when collaborative computing devices are activated.

Control Enhancements:

(1) The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use.

(2) The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers.

Enhancement Supplemental Guidance: Blocking restrictions do not include instant messaging services that are configured by an organization to perform an authorized function.

(3) The organization disables or removes collaborative computing devices from information systems in [*Assignment: organization-defined secure work areas*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** SC-15	**MOD** SC-15	**HIGH** SC-15

SC-16 TRANSMISSION OF SECURITY ATTRIBUTES

Control: The information system associates security attributes with information exchanged between information systems.

Supplemental Guidance: Security attributes may be explicitly or implicitly associated with the information contained within the information system. Related control: AC-16.

Control Enhancements:

(1) The information system validates the integrity of security attributes exchanged between systems.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES

Control: The organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.

Supplemental Guidance: For user certificates, each organization attains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice. This control focuses on certificates with a visibility external to the information system and does not include certificates related to internal system operations, for example, application-specific time services.

Control Enhancements: None.

References: OMB Memorandum 05-24; NIST Special Publications 800-32, 800-63.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-17	**HIGH** SC-17

SC-18 MOBILE CODE

Control: The organization:

a. Defines acceptable and unacceptable mobile code and mobile code technologies;

b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and

c. Authorizes, monitors, and controls the use of mobile code within the information system.

Supplemental Guidance: Decisions regarding the employment of mobile code within organizational information systems are based on the potential for the code to cause damage to the system if used maliciously. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Policy and procedures related to mobile code, address preventing the development, acquisition, or introduction of unacceptable mobile code within the information system.

Control Enhancements:

(1) The information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.

Enhancement Supplemental Guidance: Corrective actions when unauthorized mobile code is detected include, for example, blocking, quarantine, or alerting administrator. Disallowed transfers include, for example, sending word processing files with embedded macros.

(2) The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [*Assignment: organization-defined mobile code requirements*].

(3) The information system prevents the download and execution of prohibited mobile code.

(4) The information system prevents the automatic execution of mobile code in [*Assignment: organization-defined software applications*] and requires [*Assignment: organization-defined actions*] prior to executing the code.

Enhancement Supplemental Guidance: Actions required before executing mobile code, include, for example, prompting users prior to opening electronic mail attachments.

References: NIST Special Publication 800-28; DOD Instruction 8552.01.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-18	**HIGH** SC-18

SC-19 VOICE OVER INTERNET PROTOCOL

Control: The organization:

a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and

b. Authorizes, monitors, and controls the use of VoIP within the information system.

Supplemental Guidance: None.

Control Enhancements: None.

References: NIST Special Publication 800-58.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-19	**HIGH** SC-19

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.

Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to assure the authenticity and integrity of response data. The DNS security controls are consistent with, and referenced from, OMB Memorandum 08-23.

Control Enhancements:

(1) The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains.

Enhancement Supplemental Guidance: An example means to indicate the security status of child subspaces is through the use of delegation signer (DS) resource records in the DNS.

References: OMB Memorandum 08-23; NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** SC-20 (1)	**MOD** SC-20 (1)	**HIGH** SC-20 (1)

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

Control: The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems.

Supplemental Guidance: A recursive resolving or caching domain name system (DNS) server is an example of an information system that provides name/address resolution service for local clients. Authoritative DNS servers are examples of authoritative sources. Information systems that use technologies other than the DNS to map between host/service names and network addresses provide other means to enable clients to verify the authenticity and integrity of response data.

Control Enhancements:

(1) The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service.

Enhancement Supplemental Guidance: Local clients include, for example, DNS stub resolvers.

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-21

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Control: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation.

Supplemental Guidance: A domain name system (DNS) server is an example of an information system that provides name/address resolution service. To eliminate single points of failure and to enhance redundancy, there are typically at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary. Additionally, the two servers are commonly located in two different network subnets and geographically separated (i.e., not located in the same physical facility). With regard to role separation, DNS servers with an internal role, only process name/address resolution requests from within the organization (i.e., internal clients). DNS servers with an external role only process name/address resolution information requests from clients external to the organization (i.e., on the external networks including the Internet). The set of clients that can access an authoritative DNS server in a particular role is specified by the organization (e.g., by address ranges, explicit lists).

Control Enhancements: None.

References: NIST Special Publication 800-81.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-22	**HIGH** SC-22

SC-23 SESSION AUTHENTICITY

Control: The information system provides mechanisms to protect the authenticity of communications sessions.

Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).

Control Enhancements:

(1) **The information system invalidates session identifiers upon user logout or other session termination.**

(2) **The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages.**

(3) **The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.**

(4) **The information system generates unique session identifiers with [*Assignment: organization-defined randomness requirements*].**

Enhancement Supplemental Guidance: Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers.

References: NIST Special Publications 800-52, 800-77, 800-95.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-23	**HIGH** SC-23

SC-24 FAIL IN KNOWN STATE

Control: The information system fails to a [*Assignment: organization-defined known-state*] for [*Assignment: organization-defined types of failures*] preserving [*Assignment: organization-defined system state information*] in failure.

Supplemental Guidance: Failure in a known state can address safety or security in accordance with the mission/business needs of the organization. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the information system or a component of the system. Failure in a known safe state helps prevent systems from failing to a state that may cause injury to individuals or destruction to property. Preserving information system state information facilitates system restart and return to the operational mode of the organization with less disruption of mission/business processes.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SC-24

SC-25 THIN NODES

Control: The information system employs processing components that have minimal functionality and information storage.

Supplemental Guidance: The deployment of information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the need to secure every user endpoint, and may reduce the exposure of information, information systems, and services to a successful attack. Related control: SC-30.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-26 HONEYPOTS

Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks.

Supplemental Guidance: None.

Control Enhancements:

(1) The information system includes components that proactively seek to identify web-based malicious code.

Enhancement Supplemental Guidance: Devices that actively seek out web-based malicious code by posing as clients are referred to as client honeypots or honey clients.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-27 OPERATING SYSTEM-INDEPENDENT APPLICATIONS

Control: The information system includes: [*Assignment: organization-defined operating system-independent applications*].

Supplemental Guidance: Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, increasing the availability for critical functionality within an organization while information systems with a given operating system are under attack.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-28 PROTECTION OF INFORMATION AT REST

Control: The information system protects the confidentiality and integrity of information at rest.

Supplemental Guidance: This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.

Control Enhancements:

(1) **The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.**

References: NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SC-28	**HIGH** SC-28

SC-29 HETEROGENEITY

Control: The organization employs diverse information technologies in the implementation of the information system.

Supplemental Guidance: Increasing the diversity of information technologies within the information system reduces the impact of the exploitation of a specific technology. Organizations that select this control should consider that an increase in diversity may add complexity and management overhead, both of which have the potential to lead to mistakes and misconfigurations which could increase overall risk.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-30 VIRTUALIZATION TECHNIQUES

Control: The organization employs virtualization techniques to present information system components as other types of components, or components with differing configurations.

Supplemental Guidance: Virtualization techniques provide organizations with the ability to disguise information systems, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms.

Control Enhancements:

(1) The organization employs virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [*Assignment: organization-defined frequency*].

Enhancement Supplemental Guidance: While frequent changes to operating systems and applications pose configuration management challenges, the changes result in an increased work factor for adversaries in order to carry out successful attacks. Changing the apparent operating system or application, as opposed to the actual operating system or application, results in virtual changes that still impede attacker success while helping to reduce the configuration management effort.

(2) The organization employs randomness in the implementation of the virtualization techniques.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-31 COVERT CHANNEL ANALYSIS

Control: The organization requires that information system developers/integrators perform a covert channel analysis to identify those aspects of system communication that are potential avenues for covert storage and timing channels.

Supplemental Guidance: Information system developers/integrators are in the best position to identify potential avenues within the system that might lead to covert channels. Covert channel analysis is a meaningful activity when there is the potential for unauthorized information flows across security domains, for example, in the case of information systems containing export-controlled information and having connections to external networks (i.e., networks not controlled by the organization). Covert channel analysis is also meaningful in the case of multilevel secure (MLS) systems, multiple security level (MSL) systems, and cross domain systems.

Control Enhancements:

(1) The organization tests a subset of the vendor-identified covert channel avenues to determine if they are exploitable.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-32 INFORMATION SYSTEM PARTITIONING

Control: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary.

Supplemental Guidance: Information system partitioning is a part of a defense-in-depth protection strategy. An organizational assessment of risk guides the partitioning of information system components into separate physical domains (or environments). The security categorization also guides the selection of appropriate candidates for domain partitioning when system components can be associated with different system impact levels derived from the categorization. Managed interfaces restrict or prohibit network access and information flow among partitioned information system components. Related controls: AC-4, SC-7.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** SC-32	**HIGH** SC-32

SC-33 TRANSMISSION PREPARATION INTEGRITY

Control: The information system protects the integrity of information during the processes of data aggregation, packaging, and transformation in preparation for transmission.

Supplemental Guidance: Information can be subjected to unauthorized changes (e.g., malicious and/or unintentional modification) at information aggregation or protocol transformation points.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

SC-34 NON-MODIFIABLE EXECUTABLE PROGRAMS

Control: The information system at [*Assignment: organization-defined information system components*]:

a. Loads and executes the operating environment from hardware-enforced, read-only media; and

b. Loads and executes [*Assignment: organization-defined applications*] from hardware-enforced, read-only media.

Supplemental Guidance: In this control, the term operating environment is defined as the code upon which applications are hosted, for example, a monitor, executive, operating system, or application running directly on the hardware platform. Hardware-enforced, read-only media include, for example, CD-R/DVD-R disk drives. Use of non-modifiable storage ensures the integrity of the software program from the point of creation of the read-only image.

Control Enhancements:

(1) The organization employs [*Assignment: organization-defined information system components*] with no writeable storage that is persistent across component restart or power on/off.

Enhancement Supplemental Guidance: This control enhancement: (i) eliminates the possibility of malicious code insertion via persistent, writeable storage within the designated information system component; and (ii) requires no such removable storage be employed, a requirement that may be applied directly or as a specific restriction imposed through AC-19.

(2) The organization protects the integrity of the information on read-only media.

Enhancement Supplemental Guidance: This control enhancement covers protecting the integrity of information to be placed onto read-only media and controlling the media after information has been recorded onto the media. Protection measures may include, as deemed necessary by the organization, a combination of prevention and detection/response. This enhancement may be satisfied by requirements imposed by other controls such as AC-3, AC-5, CM-3, CM-5, CM-9, MP-2, MP-4, MP-5, SA-12, SC-28, SI-3, and SI-7.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

FAMILY: SYSTEM AND INFORMATION INTEGRITY **CLASS:** OPERATIONAL

SI-1 SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES

Control: The organization develops, disseminates, and reviews/updates [*Assignment: organization-defined frequency*]:

a. A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the system and information integrity family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The system and information integrity policy can be included as part of the general information security policy for the organization. System and information integrity procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the system and information integrity policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	**LOW** SI-1	**MOD** SI-1	**HIGH** SI-1

SI-2 FLAW REMEDIATION

Control: The organization:

a. Identifies, reports, and corrects information system flaws;

b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and

c. Incorporates flaw remediation into the organizational configuration management process.

Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US-

CERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.

Control Enhancements:

(1) The organization centrally manages the flaw remediation process and installs software updates automatically.

Enhancement Supplemental Guidance: Due to information system integrity and availability concerns, organizations give careful consideration to the methodology used to carry out automatic updates.

(2) The organization employs automated mechanisms [*Assignment: organization-defined frequency*] to determine the state of information system components with regard to flaw remediation.

(3) The organization measures the time between flaw identification and flaw remediation, comparing with [*Assignment: organization-defined benchmarks*].

(4) The organization employs automated patch management tools to facilitate flaw remediation to [*Assignment: organization-defined information system components*].

References: NIST Special Publication 800-40.

Priority and Baseline Allocation:

P1	**LOW** SI-2	**MOD** SI-2 (2)	**HIGH** SI-2 (1) (2)

SI-3 MALICIOUS CODE PROTECTION

Control: The organization:

a. Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:

- Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or
- Inserted through the exploitation of information system vulnerabilities;

b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;

c. Configures malicious code protection mechanisms to:

- Perform periodic scans of the information system [*Assignment: organization-defined frequency*] and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and
- [*Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator;* [*Assignment: organization-defined action*]] in response to malicious code detection; and

d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.

Control Enhancements:

(1) The organization centrally manages malicious code protection mechanisms.

(2) The information system automatically updates malicious code protection mechanisms (including signature definitions).

(3) The information system prevents non-privileged users from circumventing malicious code protection capabilities.

(4) The information system updates malicious code protection mechanisms only when directed by a privileged user.

(5) The organization does not allow users to introduce removable media into the information system.

(6) The organization tests malicious code protection mechanisms [*Assignment: organization-defined frequency*] by introducing a known benign, non-spreading test case into the information system and subsequently verifying that both detection of the test case and associated incident reporting occur, as required.

References: NIST Special Publication 800-83.

Priority and Baseline Allocation:

P1	**LOW** SI-3	**MOD** SI-3 (1) (2) (3)	**HIGH** SI-3 (1) (2) (3)

SI-4 INFORMATION SYSTEM MONITORING

Control: The organization:

a. Monitors events on the information system in accordance with [*Assignment: organization-defined monitoring objectives*] and detects information system attacks;

b. Identifies unauthorized use of the information system;

c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization;

d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and

e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations.

Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7.

Control Enhancements:

(1) The organization interconnects and configures individual intrusion detection tools into a systemwide intrusion detection system using common protocols.

(2) The organization employs automated tools to support near real-time analysis of events.

(3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination.

(4) The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.

Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.

(5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [*Assignment: organization-defined list of compromise indicators*].

Enhancement Supplemental Guidance: Alerts may be generated, depending on the organization-defined list of indicators, from a variety of sources, for example, audit records or input from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers.

(6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.

(7) The information system notifies [*Assignment: organization-defined list of incident response personnel (identified by name and/or by role)*] of suspicious events and takes [*Assignment: organization-defined list of least-disruptive actions to terminate suspicious events*].

Enhancement Supplemental Guidance: The least-disruptive actions may include initiating a request for human response.

(8) The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

(9) The organization tests/exercises intrusion-monitoring tools [*Assignment: organization-defined time-period*].

Enhancement Supplemental Guidance: The frequency of testing/exercises is dependent upon the type and method of deployment of the intrusion-monitoring tools.

(10) The organization makes provisions so that encrypted traffic is visible to information system monitoring tools.

Enhancement Supplemental Guidance: The enhancement recognizes the need to balance encrypting traffic versus the need to have insight into that traffic from a monitoring perspective. For some organizations, the need to ensure the confidentiality of traffic is paramount; for others, the mission-assurance concerns are greater.

(11) The organization analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies.

Enhancement Supplemental Guidance: Anomalies within the information system include, for example, large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

(12) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [*Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts*].

(13) The organization:

(a) Analyzes communications traffic/event patterns for the information system;

(b) Develops profiles representing common traffic patterns and/or events; and

(c) Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives to [*Assignment: organization-defined measure of false positives*] and the number of false negatives to [*Assignment: organization-defined measure of false negatives*].

(14) The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.

(15) The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.

(16) The organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness.

(17) The organization correlates results from monitoring physical, cyber, and supply chain activities to achieve integrated situational awareness.

Enhancement Supplemental Guidance: Integrated situational awareness enhances the capability of the organization to more quickly detect sophisticated attacks and investigate the methods and techniques employed to carry out the attacks.

References: NIST Special Publications 800-61, 800-83, 800-92, 800-94.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-4 (2) (4) (5) (6)	**HIGH** SI-4 (2) (4) (5) (6)

SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

Control: The organization:

a. Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;

b. Generates internal security alerts, advisories, and directives as deemed necessary;

c. Disseminates security alerts, advisories, and directives to [*Assignment: organization-defined list of personnel (identified by name and/or by role)*]; and

d. Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.

Supplemental Guidance: Security alerts and advisories are generated by the United States Computer Emergency Readiness Team (US-CERT) to maintain situational awareness across the federal government. Security directives are issued by OMB or other designated organizations with the responsibility and authority to issue such directives. Compliance to security directives is *essential* due to the critical nature of many of these directives and the potential immediate adverse affects on organizational operations and assets, individuals, other organizations, and the Nation should the directives not be implemented in a timely manner.

Control Enhancements:

(1) The organization employs automated mechanisms to make security alert and advisory information available throughout the organization as needed.

References: NIST Special Publication 800-40.

Priority and Baseline Allocation:

P1	**LOW** SI-5	**MOD** SI-5	**HIGH** SI-5 (1)

SI-6 SECURITY FUNCTIONALITY VERIFICATION

Control: The information system verifies the correct operation of security functions [*Selection (one or more):* [*Assignment: organization-defined system transitional states*]; *upon command by user with appropriate privilege; periodically every* [*Assignment: organization-defined time-period*]] and [*Selection (one or more): notifies system administrator; shuts the system down; restarts the system;* [*Assignment: organization-defined alternative action(s)*]] when anomalies are discovered.

Supplemental Guidance: The need to verify security functionality applies to all security functions. For those security functions that are not able to execute automated self-tests, the organization either implements compensating security controls or explicitly accepts the risk of not performing the verification as required. Information system transitional states include, for example, startup, restart, shutdown, and abort.

Control Enhancements:

(1) The information system provides notification of failed automated security tests.

(2) The information system provides automated support for the management of distributed security testing.

(3) The organization reports the result of security function verification to designated organizational officials with information security responsibilities.

Enhancement Supplemental Guidance: Organizational officials with information security responsibilities include, for example, senior information security officers, information system security managers, and information systems security officers.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** Not Selected	**HIGH** SI-6

SI-7 SOFTWARE AND INFORMATION INTEGRITY

Control: The information system detects unauthorized changes to software and information.

Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.

Control Enhancements:

(1) The organization reassesses the integrity of software and information by performing [*Assignment: organization-defined frequency*] integrity scans of the information system.

(2) The organization employs automated tools that provide notification to designated individuals upon discovering discrepancies during integrity verification.

(3) The organization employs centrally managed integrity verification tools.

(4) The organization requires use of tamper-evident packaging for [*Assignment: organization-defined information system components*] during [*Selection: transportation from vendor to operational site; during operation; both*].

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-7 (1)	**HIGH** SI-7 (1) (2)

SI-8 SPAM PROTECTION

Control: The organization:

a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and

b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.

Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.

Control Enhancements:

(1) The organization centrally manages spam protection mechanisms.

(2) The information system automatically updates spam protection mechanisms (including signature definitions).

References: NIST Special Publication 800-45.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-8	**HIGH** SI-8 (1)

SI-9 INFORMATION INPUT RESTRICTIONS

Control: The organization restricts the capability to input information to the information system to authorized personnel.

Supplemental Guidance: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SI-9	**HIGH** SI-9

SI-10 INFORMATION INPUT VALIDATION

Control: The information system checks the validity of information inputs.

Supplemental Guidance: Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P1	**LOW** Not Selected	**MOD** SI-10	**HIGH** SI-10

SI-11 ERROR HANDLING

Control: The information system:

a. Identifies potentially security-relevant error conditions;

b. Generates error messages that provide information necessary for corrective actions without revealing [*Assignment: organization-defined sensitive or potentially harmful information*] in error logs and administrative messages that could be exploited by adversaries; and

c. Reveals error messages only to authorized personnel.

Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** Not Selected	**MOD** SI-11	**HIGH** SI-11

SI-12 INFORMATION OUTPUT HANDLING AND RETENTION

Control: The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

Supplemental Guidance: The output handling and retention requirements cover the full life cycle of the information, in some cases extending beyond the disposal of the information system. The National Archives and Records Administration provides guidance on records retention. Related controls: MP-2, MP-4.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

P2	**LOW** SI-12	**MOD** SI-12	**HIGH** SI-12

SI-13 PREDICTABLE FAILURE PREVENTION

Control: The organization:

a. Protects the information system from harm by considering mean time to failure for [*Assignment: organization-defined list of information system components*] in specific environments of operation; and

b. Provides substitute information system components, when needed, and a mechanism to exchange active and standby roles of the components.

Supplemental Guidance: While mean time to failure is primarily a reliability issue, this control focuses on the potential failure of specific components of the information system that provide security capability. Mean time to failure rates are defendable and based on considerations that are installation-specific, not industry-average. The transfer of responsibilities between active and standby information system components does not compromise safety, operational readiness, or security (e.g., state variables are preserved). The standby component is available at all times except where a failure recovery is in progress or for maintenance reasons. Related control: CP-2.

Control Enhancements:

(1) The organization takes the information system component out of service by transferring component responsibilities to a substitute component no later than [*Assignment: organization-defined fraction or percentage*] of mean time to failure.

(2) The organization does not allow a process to execute without supervision for more than [*Assignment: organization-defined time period*].

(3) The organization manually initiates a transfer between active and standby information system components at least once per [*Assignment: organization-defined frequency*] if the mean time to failure exceeds [*Assignment: organization-defined time period*].

(4) The organization, if an information system component failure is detected:

(a) Ensures that the standby information system component successfully and transparently assumes its role within [*Assignment: organization-defined time period*]; and

(b) [*Selection (one or more): activates* [*Assignment: organization-defined alarm*]; *automatically shuts down the information system*].

Enhancement Supplemental Guidance: Automatic or manual transfer of roles to a standby unit may occur upon detection of a component failure.

References: None.

Priority and Baseline Allocation:

P0	**LOW** Not Selected	**MOD** Not Selected	**HIGH** Not Selected

APPENDIX G

INFORMATION SECURITY PROGRAMS

ORGANIZATION-WIDE INFORMATION SECURITY PROGRAM MANAGEMENT CONTROLS

The Federal Information Security Management Act (FISMA) requires organizations to develop and implement an organization-wide information security program to address information security for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, contractor, or other source. The information security program management (PM) controls described in this appendix complement the security controls in Appendix F and focus on the organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Organizations specify the individuals within the organization responsible for the development, implementation, assessment, authorization, and monitoring of the information security program management controls. Organizations document program management controls in the *information security program plan*. The organization-wide information security program plan supplements the individual security plans developed for each organizational information system. Together, the security plans for the individual information systems and the information security program cover the totality of security controls employed by the organization.

In addition to documenting the information security program management controls, the security program plan provides a vehicle for the organization, in a central repository, to document all security controls from Appendix F that have been designated as *common controls* (i.e., security controls inherited by organizational information systems). The information security program management controls and common controls contained in the information security program plan are implemented, assessed for effectiveness,[74] and authorized by a senior organizational official, with the same or similar authority and responsibility for managing risk as the authorization officials for information systems.[75] Plans of action and milestones are developed and maintained for the program management and common controls that are deemed through assessment to be less than effective. Information security program management and common controls are also subject to the same continuous monitoring requirements as security controls employed in individual organizational information systems.

Cautionary Note

Organizations are required to implement security program management controls to provide a foundation for the organization's information security program. The successful implementation of security controls for organizational information systems depends on the successful implementation of the organization's program management controls.

[74] Assessment procedures for program management controls and common controls can be found in NIST Special Publication 800-53A.

[75] In situations where common controls are inherited from external environments, organizations should consult the guidance provided in Section 3.4.

PM-1 INFORMATION SECURITY PROGRAM PLAN

Control: The organization:

a. Develops and disseminates an organization-wide information security program plan that:

- Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
- Provides sufficient information about the program management controls and common controls (including specification of parameters for any *assignment* and *selection* operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended;
- Includes roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
- Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;

b. Reviews the organization-wide information security program plan [*Assignment: organization-defined frequency*]; and

c. Revises the plan to address organizational changes and problems identified during plan implementation or security control assessments.

Supplemental Guidance: The information security program plan can be represented in a single document or compilation of documents at the discretion of the organization. The plan documents the organization-wide program management controls and organization-defined common controls. The security plans for individual information systems and the organization-wide information security program plan together, provide complete coverage for all security controls employed within the organization. Common controls are documented in an appendix to the organization's information security program plan unless the controls are included in a separate security plan for an information system (e.g., security controls employed as part of an intrusion detection system providing organization-wide boundary protection inherited by one or more organizational information systems). The organization-wide information security program plan will indicate which separate security plans contain descriptions of common controls.

Organizations have the flexibility to describe common controls in a single document or in multiple documents. In the case of multiple documents, the documents describing common controls are included as attachments to the information security program plan. If the information security program plan contains multiple documents, the organization specifies in each document the organizational official or officials responsible for the development, implementation, assessment, authorization, and monitoring of the respective common controls. For example, the organization may require that the Facilities Management Office develop, implement, assess, authorize, and continuously monitor common physical and environmental protection controls from the PE family when such controls are not associated with a particular information system but instead, support multiple information systems. Related control: PM-8.

Control Enhancements: None.

References: None.

PM-2 SENIOR INFORMATION SECURITY OFFICER

Control: The organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.

Supplemental Guidance: The security officer described in this control is an organizational official. For a federal agency (as defined in applicable federal laws, Executive Orders, directives, policies, or regulations) this official is the Senior Agency Information Security Officer. Organizations may also refer to this organizational official as the Senior Information Security Officer or Chief Information Security Officer.

Control Enhancements: None.

References: None.

PM-3 INFORMATION SECURITY RESOURCES

Control: The organization:

a. Ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement;

b. Employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and

c. Ensures that information security resources are available for expenditure as planned.

Supplemental Guidance: Organizations may designate and empower an Investment Review Board (or similar group) to manage and provide oversight for the information security-related aspects of the capital planning and investment control process. Related controls: PM-4, SA-2.

Control Enhancements: None.

References: NIST Special Publication 800-65.

PM-4 PLAN OF ACTION AND MILESTONES PROCESS

Control: The organization implements a process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions to mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The plan of action and milestones is a key document in the information security program and is subject to federal reporting requirements established by OMB. The plan of action and milestones updates are based on the findings from security control assessments, security impact analyses, and continuous monitoring activities. OMB FISMA reporting guidance contains instructions regarding organizational plans of action and milestones. Related control: CA-5.

Control Enhancements: None.

References: OMB Memorandum 02-01; NIST Special Publication 800-37.

PM-5 INFORMATION SYSTEM INVENTORY

Control: The organization develops and maintains an inventory of its information systems.

Supplemental Guidance: This control addresses the inventory requirements in FISMA. OMB provides guidance on developing information systems inventories and associated reporting requirements.

Control Enhancements: None.

References: None.

PM-6 INFORMATION SECURITY MEASURES OF PERFORMANCE

Control: The organization develops, monitors, and reports on the results of information security measures of performance.

Supplemental Guidance: Measures of performance are outcome-based metrics used by an organization to measure the effectiveness or efficiency of the information security program and the security controls employed in support of the program.

Control Enhancements: None.

References: NIST Special Publication 800-55.

PM-7 ENTERPRISE ARCHITECTURE

Control: The organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Supplemental Guidance: The enterprise architecture developed by the organization is aligned with the Federal Enterprise Architecture. The integration of information security requirements and associated security controls into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the system development life cycle and are directly and explicitly related to the organization's mission/business processes. This also embeds into the enterprise architecture, an integral security architecture consistent with organizational risk management and information security strategies. Security requirements and control integration are most effectively accomplished through the application of the Risk Management Framework and supporting security standards and guidelines. The Federal Segment Architecture Methodology provides guidance on integrating information security requirements and security controls into enterprise architectures. Related controls: PL-2, PM-11, RA-2.

Control Enhancements: None.

References: NIST Special Publication 800-39; Web: WWW.FSAM.GOV.

PM-8 CRITICAL INFRASTRUCTURE PLAN

Control: The organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Supplemental Guidance: The requirement and guidance for defining critical infrastructure and key resources and for preparing an associated critical infrastructure protection plan are found in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Related controls: PM-1, PM-9, PM-11, RA-3.

Control Enhancements: None.

References: HSPD 7.

PM-9 RISK MANAGEMENT STRATEGY

Control: The organization:

a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and

b. Implements that strategy consistently across the organization.

Supplemental Guidance: An organization-wide risk management strategy includes, for example, an unambiguous expression of the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time. The use of a risk executive function can facilitate consistent, organization-wide application of the risk management strategy. The organization-wide risk management strategy can be informed by risk-related inputs from other sources both internal and external to the organization to ensure the strategy is both broad-based and comprehensive. Related control: RA-3.

Control Enhancements: None.

References: NIST Special Publications 800-30, 800-39.

PM-10 SECURITY AUTHORIZATION PROCESS

Control: The organization:

a. Manages (i.e., documents, tracks, and reports) the security state of organizational information systems through security authorization processes;

b. Designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and

c. Fully integrates the security authorization processes into an organization-wide risk management program.

Supplemental Guidance: The security authorization process for information systems requires the implementation of the Risk Management Framework and the employment of associated security standards and guidelines. Specific roles within the risk management process include a designated authorizing official for each organizational information system. Related control: CA-6.

Control Enhancements: None.

References: NIST Special Publications 800-37, 800-39.

PM-11 MISSION/BUSINESS PROCESS DEFINITION

Control: The organization:

a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and

b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.

Supplemental Guidance: Information protection needs are technology-independent, required capabilities to counter threats to organizations, individuals, or the Nation through the compromise of information (i.e., loss of confidentiality, integrity, or availability). Information protection needs are derived from the mission/business needs defined by the organization, the mission/business processes selected to meet the stated needs, and the organizational risk management strategy. Information protection needs determine the required security controls for the organization and the associated information systems supporting the mission/business processes. Inherent in defining an organization's information protection needs is an understanding of the level of adverse impact that could result if a compromise of information occurs. The security categorization process is used to make such potential impact determinations. Mission/business process definitions and associated information protection requirements are documented by the organization in accordance with organizational policy and procedure. Related controls: PM-7, PM-8, RA-2.

Control Enhancements: None.

References: FIPS Publication 199; NIST Special Publication 800-60.

APPENDIX H

INTERNATIONAL INFORMATION SECURITY STANDARDS

SECURITY CONTROL MAPPINGS FOR ISO/IEC 27001

The mapping tables in this appendix provide organizations with a *general* indication of security control coverage with respect to ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements*.[76] ISO/IEC 27001 applies to all types of organizations (e.g., commercial, government) and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system (ISMS) within the context of the organization's overall business risks. While the risk management approach established by NIST originally focused on managing risk from information systems (as required by FISMA and described in NIST Special Publication 800-39), the approach is being expanded to include risk management at the organizational level. A forthcoming version of NIST Special Publication 800-39 will incorporate ISO/IEC 27001 to manage organizational information security risk through the establishment of an ISMS. Since NIST's mission includes the adoption of international and national standards where appropriate, NIST intends to pursue convergence to reduce the burden on organizations that must conform to both sets of standards. The convergence initiative will be carried out in three phases. Phase I, the subject of this appendix, provides a two-way mapping between the security controls in NIST Special Publication 800-53 and the controls in ISO/IEC 27001 (Annex A). Phase II will provide a two-way mapping between the organization-level risk management concepts in NIST Special Publication 800-39 (forthcoming version) and general requirements in ISO/IEC 27001. Phase III will use the results from Phase I and II to fully integrate ISO/IEC 27001 into NIST's risk management approach such that an organization that complies with NIST standards and guidelines can also comply with ISO/IEC 27001 (subject to appropriate assessment requirements for ISO/IEC 27001 certification).

Table H-1 provides a forward mapping from the security controls in NIST Special Publication 800-53 to the controls in ISO/IEC 27001 (Annex A). The mappings are created by using the primary security topic identified in each of the Special Publication 800-53 security controls and associated control enhancements (if any) and searching for a similar security topic in ISO/IEC 27001 (Annex A). Security controls with similar functional meaning are included in the mapping table. For example, Special Publication 800-53 contingency planning and ISO/IEC 27001 (Annex A) business continuity were deemed to have similar, but not the same, functionality. In some cases, similar topics are addressed in the security control sets but provide a different context, perspective, or scope. For example, Special Publication 800-53 addresses information flow control broadly in terms of approved authorizations for controlling access between source and destination objects, whereas ISO/IEC 27001 (Annex A) addresses the information flow more narrowly as it applies to interconnected network domains. Table H-2 provides a reverse mapping from the security controls in ISO/IEC 27001 (Annex A) to the security controls in Special Publication 800-53.[77]

[76] ISO/IEC 27001 was published in October 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[77] The use of the term *XX-1 controls* in mapping Table H-2 refers to the set of security controls represented by the first control in each family in NIST Special Publication 800-53, where *XX* is a placeholder for the two-letter family identifier. These security controls primarily focus on policies and procedures for each topic area addressed by the respective security control family.

Organizations are encouraged to use the mapping tables as a starting point for conducting further analyses and interpretation of the extent of compliance with ISO/IEC 27001 from compliance with the NIST security standards and guidelines and visa versa. Organizations that use the security controls in Special Publication 800-53 as an extension to the security controls in Annex A in their ISO/IEC 27001 implementations will have a higher probability of complying with NIST security standards and guidelines than those organizations that use only Annex A.

TABLE H-1: MAPPING NIST SP 800-53 TO ISO/IEC 27001 (ANNEX A)

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
AC-1	Access Control Policy and Procedures	A5.1.1, A5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A10.1.1, A.10.8.1, A.11.1.1, A.11.2.1, A11.2.2, A11.4.1, A.11.7.1, A.11.7.2, A.15.1.1, A.15.2.1
AC-2	Account Management	A.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A15.2.1
AC-3	Access Enforcement	A.10.8.1 A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.2
AC-4	Information Flow Enforcement	A.10.6.1, A.10.8.1, A.11.4.5, A.11.4.7, A.11.7.2, A.12.4.2, A.12.5.4
AC-5	Separation of Duties	A.6.1.3, A.8.1.1, A.10.1.3, A.11.1.1, A.11.4.1
AC-6	Least Privilege	A.6.1.3, A.8.1.1, A.11.1.1, A.11.2.2, A.11.4.1, A.11.4.4, A.11.4.6, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Login Attempts	A.11.5.1
AC-8	System Use Notification	A.6.2.2, A.8.1.1, A.11.5.1, A.15.1.5
AC-9	Previous Logon (Access) Notification	A.11.5.1
AC-10	Concurrent Session Control	A.11.5.1
AC-11	Session Lock	A.11.3.2, A.11.3.3, A.11.5.5
AC-12	**Withdrawn**	---
AC-13	**Withdrawn**	---
AC-14	Permitted Actions without Identification or Authentication	A.11.6.1
AC-15	**Withdrawn**	---
AC-16	Security Attributes	A.7.2.2
AC-17	Remote Access	A.10.6.1, A.10.8.1, A.11.1.1, A.11.4.1, A.11.4.2, A.11.4.4, A.11.4.6, A.11.4.7, A.11.7.1, A.11.7.2
AC-18	Wireless Access	A.10.6.1, A.10.8.1, A.11.1.1, A.11.4.1, A.11.4.2, A.11.4.4, A.11.4.6, A.11.4.7, A.11.7.1, A.11.7.2
AC-19	Access Control for Mobile Devices	A.10.4.1, A.11.1.1, A.11.4.3, A.11.7.1
AC-20	Use of External Information Systems	A.7.1.3, A.8.1.1, A.8.1.3, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2
AC-21	User-Based Collaboration and Information Sharing	A.11.2.1, A.11.2.2
AC-22	Publicly Accessible Content	None
AT-1	Security Awareness and Training Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
AT-2	Security Awareness	A.6.2.2, A.8.1.1, A.8.2.2, A.9.1.5, A.10.4.1
AT-3	Security Training	A.8.1.1, A.8.2.2, A.9.1.5
AT-4	Security Training Records	None
AT-5	Contacts with Security Groups and Associations	A.6.1.7
AU-1	Audit and Accountability Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.10.2, A.15.1.1, A.15.2.1, A.15.3.1
AU-2	Auditable Events	A.10.10.1, A.10.10.4, A.10.10.5, A.15.3.1
AU-3	Content of Audit Records	A.10.10.1
AU-4	Audit Storage Capacity	A.10.10.1, A.10.3.1
AU-5	Response to Audit Processing Failures	A.10.3.1, A.10.10.1
AU-6	Audit Review, Analysis, and Reporting	A.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5
AU-7	Audit Reduction and Report Generation	A.10.10.2
AU-8	Time Stamps	A.10.10.1, A.10.10.6
AU-9	Protection of Audit Information	A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2
AU-10	Non-repudiation	A.10.9.1, A.12.2.3
AU-11	Audit Record Retention	A.10.10.1, A.10.10.2, A.15.1.3

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
AU-12	Audit Generation	A.10.10.1, A.10.10.4, A.10.10.5
AU-13	Monitoring for Information Disclosure	None
AU-14	Session Audit	None
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.6.1.4, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
CA-2	Security Assessments	A.6.1.8, A.10.3.2, A.15.2.1, A.15.2.2
CA-3	Information System Connections	A.6.2.1, A.6.2.3, A.10.6.1, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring	A.6.1.8, A.15.2.1, A.15.2.2
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.1.2, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1
CM-2	Baseline Configuration	A.12.4.1, A.10.1.4
CM-3	Configuration Change Control	A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3
CM-4	Security Impact Analysis	A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change	A.10.1.2, A.11.1.1, A.11.6.1, A.12.4.1, A.12.4.3, A.12.5.3
CM-6	Configuration Settings	None
CM-7	Least Functionality	None
CM-8	Information System Component Inventory	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan	A.6.1.3. A.7.1.1, A.7.1.2, A.8.1.1, A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3
CP-1	Contingency Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.10.1.1, A.10.1.2, A.14.1.1, A.14.1.3, A.15.1.1, A.15.2.1
CP-2	Contingency Plan	A.6.1.2, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5
CP-3	Contingency Training	A.8.2.2, A.9.1.4, A.14.1.3
CP-4	Contingency Plan Testing and Exercises	A.6.1.2, A.9.1.4, A.14.1.1, A.14.1.3, A.14.1.4, A.14.1.5
CP-5	**Withdrawn**	---
CP-6	Alternate Storage Site	A.9.1.4, A.14.1.3
CP-7	Alternate Processing Site	A.9.1.4, A.14.1.3
CP-8	Telecommunications Services	A.9.1.4, A.10.6.1, A.14.1.3
CP-9	Information System Backup	A.9.1.4, A.10.5.1, A.14.1.3, A.15.1.3
CP-10	Information System Recovery and Reconstitution	A.9.1.4, A.14.1.3
IA-1	Identification and Authentication Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.11.2.1, A.15.1.1, A.15.2.1
IA-2	Identification and Authentication (Organizational Users)	A.11.3.2, A.11.5.1, A.11.5.2, A.11.5.3
IA-3	Device Identification and Authentication	A.11.4.3
IA-4	Identifier Management	A.11.5.2
IA-5	Authenticator Management	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.2, A.11.5.3
IA-6	Authenticator Feedback	A.11.5.1
IA-7	Cryptographic Module Authentication	A.12.3.1, A.15.1.1, A.15.1.6, A.15.2.1
IA-8	Identification and Authentication (Non-Organizational Users)	A.10.9.1, A.11.4.2, A.11.5.1, A.11.5.2
IR-1	Incident Response Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1
IR-2	Incident Response Training	A.8.2.2
IR-3	Incident Response Testing and Exercises	None
IR-4	Incident Handling	A.6.1.2, A.13.2.2, A.13.2.3
IR-5	Incident Monitoring	None
IR-6	Incident Reporting	A.6.1.6, A.13.1.1
IR-7	Incident Response Assistance	None
IR-8	Incident Response Plan	None
MA-1	System Maintenance Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.2.4, A.10.1.1, A.15.1.1, A.15.2.1
MA-2	Controlled Maintenance	A.9.2.4

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
MA-3	Maintenance Tools	A.9.2.4, A.11.4.4
MA-4	Non-Local Maintenance	A.9.2.4, A.11.4.4
MA-5	Maintenance Personnel	A.9.2.4, A.12.4.3
MA-6	Timely Maintenance	A.9.2.4
MP-1	Media Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.10.7.2, A.10.7.3, A.11.1.1, A.15.1.1, A.15.1.3, A.15.2.1
MP-2	Media Access	A.7.2.2, A.10.7.1, A.10.7.3
MP-3	Media Marking	A.7.2.2, A.10.7.1, A.10.7.3
MP-4	Media Storage	A.10.7.1, A.10.7.3, A.10.7.4, A.15.1.3
MP-5	Media Transport	A.9.2.5, A.9.2.7, A.10.7.1, A.10.7.3, A.10.8.3
MP-6	Media Sanitization	A.9.2.6, A.10.7.1, A.10.7.2, A.10.7.3
PE-1	Physical and Environmental Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.9.1.4, A.9.2.1, A.9.2.2, A.10.1.1, A.11.1.1, A.11.2.1, A.11.2.2, A.15.1.1, A.15.2.1
PE-2	Physical Access Authorizations	A.9.1.5, A.11.2.1, A.11.2.2, A.11.2.4
PE-3	Physical Access Control	A.9.1.1, A.9.1.2, A.9.1.3, A.9.1.5, A.9.1.6, A.11.3.2, A.11.4.4
PE-4	Access Control for Transmission Medium	A.9.1.3, A.9.1.5, A.9.2.3
PE-5	Access Control for Output Devices	A.9.1.2, A.9.1.3, A.10.6.1, A.11.3.2
PE-6	Monitoring Physical Access	A.9.1.2, A.9.1.5, A.10.10.2
PE-7	Visitor Control	A.9.1.2, A.9.1.5, A.9.1.6
PE-8	Access Records	A.9.1.5, A.10.10.2, A.15.2.1
PE-9	Power Equipment and Power Cabling	A.9.1.4, A.9.2.2, A.9.2.3
PE-10	Emergency Shutoff	A.9.1.4
PE-11	Emergency Power	A.9.1.4, A.9.2.2
PE-12	Emergency Lighting	A.9.2.2
PE-13	Fire Protection	A.9.1.4
PE-14	Temperature and Humidity Controls	A.9.2.2
PE-15	Water Damage Protection	A.9.1.4
PE-16	Delivery and Removal	A.9.1.6, A.9.2.7, A.10.7.1
PE-17	Alternate Work Site	A.9.2.5, A.11.7.2
PE-18	Location of Information System Components	A.9.2.1, A.11.3.2
PE-19	Information Leakage	A.12.5.4
PL-1	Security Planning Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PL-2	System Security Plan	None
PL-3	**Withdrawn**	---
PL-4	Rules of Behavior	A.6.1.5, A.6.2.2, A.7.1.3. A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.12.4.1, A.13.1.2, A.15.1.5
PL-5	Privacy Impact Assessment	A.15.1.4
PL-6	Security-Related Activity Planning	A.6.1.2, A.15.3.1
PS-1	Personnel Security Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
PS-2	Position Categorization	A.8.1.1
PS-3	Personnel Screening	A.8.1.2
PS-4	Personnel Termination	A.8.3.1, A.8.3.2, A.8.3.3
PS-5	Personnel Transfer	A.8.3.1, A.8.3.2, A.8.3.3
PS-6	Access Agreements	A.6.1.5, A.8.1.1, A.8.1.3, A.8.2.1, A.9.1.5, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5
PS-7	Third-Party Personnel Security	A.6.2.3, A.8.1.1, A.8.2.1, A.8.1.3
PS-8	Personnel Sanctions	A.8.2.3, A.15.1.5
RA-1	Risk Assessment Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.14.1.2, A.15.1.1, A.15.2.1
RA-2	Security Categorization	A.7.2.1, A.14.1.2
RA-3	Risk Assessment	A.6.2.1, A.10.2.3, A.12.6.1, A.14.1.2
RA-4	**Withdrawn**	---
RA-5	Vulnerability Scanning	A.12.6.1, A.15.2.2
SA-1	System and Services Acquisition Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.6.2.1, A.8.1.1, A.10.1.1, A.12.1.1, A.12.5.5, A.15.1.1, A.15.2.1
SA-2	Allocation of Resources	A.6.1.2, A.10.3.1

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
SA-3	Life Cycle Support	A.12.1.1
SA-4	Acquisitions	A.12.1.1, A.12.5.5
SA-5	Information System Documentation	A.10.7.4, A.15.1.3
SA-6	Software Usage Restrictions	A.12.4.1, A.12.5.5, A.15.1.2
SA-7	User-Installed Software	A.12.4.1, A.12.5.5, A.15.1.5
SA-8	Security Engineering Principles	A.10.4.1, A.10.4.2, A.11.4.5, A.12.5.5
SA-9	External Information System Services	A.6.1.5, A.6.2.1, A.6.2.3, A.8.1.1, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5
SA-10	Developer Configuration Management	A.12.4.3, A.12.5.1, A.12.5.5
SA-11	Developer Security Testing	A.10.3.2, A.12.5.5
SA-12	Supply Chain Protections	A.12.5.5
SA-13	Trustworthiness	A.12.5.5
SA-14	Critical Information System Components	None
SC-1	System and Communications Protection Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SC-2	Application Partitioning	A.10.4.1, A.10.4.2
SC-3	Security Function Isolation	A.10.4.1, A.10.4.2, A.10.9.1, A.10.9.2
SC-4	Information In Shared Resources	None
SC-5	Denial of Service Protection	A.10.3.1
SC-6	Resource Priority	None
SC-7	Boundary Protection	A.6.2.1, A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.5, A.11.4.6
SC-8	Transmission Integrity	A.10.4.2, A.10.6.1, A.10.6.2, A.10.9.1, A.10.9.2, A.12.2.3, A.12.3.1
SC-9	Transmission Confidentiality	A.10.6.1, A.10.6.2, A.10.9.1, A.10.9.2, A.12.3.1
SC-10	Network Disconnect	A.10.6.1, A.11.3.2, A.11.5.1, A.11.5.5
SC-11	Trusted Path	None
SC-12	Cryptographic Key Establishment and Management	A.12.3.2
SC-13	Use of Cryptography	A.12.3.1, A.15.1.6
SC-14	Public Access Protections	A.10.4.1, A.10.4.2, A.10.9.1, A.10.9.2, A.10.9.3
SC-15	Collaborative Computing Devices	None
SC-16	Transmission of Security Attributes	A.7.2.2, A.10.8.1
SC-17	Public Key Infrastructure Certificates	A.12.3.2
SC-18	Mobile Code	A.10.4.2
SC-19	Voice Over Internet Protocol	A.10.6.1
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	A.10.6.1
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	A.10.6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service	A.10.6.1
SC-23	Session Authenticity	A.10.6.1
SC-24	Fail in Known State	None
SC-25	Thin Nodes	None
SC-26	Honeypots	None
SC-27	Operating System-Independent Applications	None
SC-28	Protection of Information at Rest	None
SC-29	Heterogeneity	None
SC-30	Virtualization Techniques	None
SC-31	Covert Channel Analysis	None
SC-32	Information System Partitioning	None
SC-33	Transmission Preparation Integrity	None
SC-34	Non-Modifiable Executable Programs	None
SI-1	System and Information Integrity Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
SI-2	Flaw Remediation	A.10.10.5, A.12.5.2, A.12.6.1, A.13.1.2
SI-3	Malicious Code Protection	A.10.4.1
SI-4	Information System Monitoring	A.10.10.2, A.13.1.1, A.13.1.2

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
SI-5	Security Alerts, Advisories, and Directives	A.6.1.6, A.12.6.1, A.13.1.1, A.13.1.2
SI-6	Security Functionality Verification	None
SI-7	Software and Information Integrity	A.10.4.1, A.12.2.2, A.12.2.3
SI-8	Spam Protection	None
SI-9	Information Input Restrictions	A.10.8.1, A.11.1.1, A.11.2.2, A.12.2.2
SI-10	Information Input Validation	A.12.2.1, A.12.2.2
SI-11	Error Handling	None
SI-12	Information Output Handling and Retention	A.10.7.3, A.15.1.3, A.15.1.4, A.15.2.1
SI-13	Predictable Failure Prevention	None
PM-1	Information Security Program Plan	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.8.1.1, A.15.1.1, A.15.2.1
PM-2	Senior Information Security Officer	A.6.1.1, A.6.1.2, A.6.1.3
PM-3	Information Security Resources	None
PM-4	Plan of Action and Milestones Process	None
PM-5	Information System Inventory	A.7.1.1, A.7.1.2
PM-6	Information Security Measures of Performance	None
PM-7	Enterprise Architecture	None
PM-8	Critical Infrastructure Plan	None
PM-9	Risk Management Strategy	A.6.2.1, A.14.1.2
PM-10	Security Authorization Process	A.6.1.4
PM-11	Mission/Business Process Definition	None

TABLE H-2: MAPPING ISO/IEC 27001 (ANNEX A) TO NIST SP 800-53

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.5 Security Policy	
A.5.1 Information security policy	
A.5.1.1 Information security policy document	XX-1 controls
A.5.1.2 Review of the information security policy	XX-1 controls
A.6 Organization of information security	
A.6.1 Internal	
A.6.1.1 Management commitment to information security	XX-1 controls, PM-2; SP 800-39, SP 800-37
A.6.1.2 Information security coordination	CP-2, CP-4, IR-4, PL-1, PL-6, PM-2, SA-2; SP 800-39, SP 800-37
A.6.1.3 Allocation of information security responsibilities	XX-1 controls, AC-5, AC-6, CM-9. PM-2; SP 800-39, SP 800-37
A.6.1.4 Authorization process for information processing facilities	CA-1, CA-6, PM-10; SP 800-37
A.6.1.5 Confidentiality agreements	PL-4, PS-6, SA-9
A.6.1.6 Contact with authorities	Multiple controls with contact reference (e.g., IR-6, SI-5); SP 800-39; SP 800-37
A.6.1.7 Contact with special interest groups	AT-5
A.6.1.8 Independent review of information security	CA-2, CA-7; SP 800-39, SP 800-37
A.6.2 External Parties	
A.6.2.1 Identification of risks related to external parties	CA-3, PM-9, RA-3, SA-1, SA-9, SC-7
A.6.2.2 Addressing security when dealing with customers	AC-8 , AT-2, PL-4
A.6.2.3 Addressing security in third party agreements	CA-3, PS-7, SA-9
A.7 Asset Management	
A.7.1 Responsibility for assets	
A.7.1.1 Inventory of assets	CM-8, CM-9, PM-5
A.7.1.2 Ownership of assets	CM-8, CM-9, PM-5
A.7.1.3 Acceptable use of assets	AC-20, PL-4
A.7.2 Information Classification	
A.7.2.1 Classification Guidelines	RA-2
A.7.2.2 Information labeling and handling	AC-16, MP-2, MP-3, SC-16
A.8 Human Resources Security	
A.8.1 Prior to Employment	
A.8.1.1 Roles and Responsibilities	XX-1 controls, AC-5, AC-6, AC-8, AC-20, AT-2, AT-3, CM-9, PL-4, PS-2, PS-6, PS-7, SA-9
A.8.1.2 Screening	PS-3
A.8.1.3 Terms and conditions of employment	AC-20, PL-4, PS-6, PS-7
A.8.2 During employment	
A.8.2.1 Management responsibilities	PL-4, PS-6, PS-7, SA-9
A.8.2.2 Awareness, education, and training	AT-2, AT-3, IR-2
A.8.2.3 Disciplinary process	PS-8
A.8.3 Termination or change of employment	
A.8.3.1 Termination responsibilities	PS-4, PS-5
A.8.3.2 Return of assets	PS-4, PS-5
A.8.3.3 Removal of access rights	AC-2, PS-4, PS-5
A.9 Physical and environmental security	
A.9.1 Secure areas	
A.9.1.1 Physical security perimeter	PE-3
A.9.1.2 Physical entry controls	PE-3, PE-5, PE-6, PE-7
A.9.1.3 Securing offices, rooms, facilities	PE-3, PE-4, PE-5
A.9.1.4 Protecting against external and environmental threats	CP Family; PE-1, PE-9, PE-10, PE-11, PE-13, PE-15
A.9.1.5 Working in secure areas	AT-2, AT-3 , PL-4, PS-6, PE-2, PE-3, PE-4, PE-6, PE-7, PE-8
A.9.1.6 Public access, delivery and loading areas	PE-3 , PE-7, PE-16
A.9.2 Equipment security	
A.9.2.1 Equipment siting and protection	PE-1, PE-18
A.9.2.2 Supporting utilities	PE-1, PE-9, PE-11, PE-12, PE-14
A.9.2.3 Cabling security	PE-4, PE-9
A.9.2.4 Equipment maintenance	MA Family

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.9.2.5 Security of equipment off-premises	MP-5, PE-17
A.9.2.6 Secure disposal or reuse of equipment	MP-6
A.9.2.7 Removal of property	MP-5, PE-16
A.10 Communications and operations management	
A.10.1 Operational procedures and responsibilities	
A.10.1.1 Documented operating procedures	XX-1 controls, CM-9
A.10.1.2 Change management	CM-1, CM-3, CM-4, CM-5, CM-9
A.10.1.3 Segregation of duties	AC-5
A.10.1.4 Separation of development, test and operational facilities	CM-2
A.10.2 Third-party service delivery management	
A.10.2.1 Service delivery	SA-9
A.10.2.2 Monitoring and review of third-party services	SA-9
A.10.2.3 Managing changes to third-party services	RA-3, SA-9
A.10.3 System planning and acceptance	
A.10.3.1 Capacity management	AU-4, AU-5, CP-2, SA-2, SC-5
A.10.3.2 System acceptance	CA-2, CA-6, CM-3, CM-4, CM-9, SA-11
A.10.4 Protection against malicious and mobile code	
A.10.4.1 Controls against malicious code	AC-19, AT-2, SA-8, SC-2, SC-3, SC-7, SC-14, SI-3, SI-7
A.10.4.2 Controls against mobile code	SA-8, SC-2, SC-3, SC-7, SC-14, SC-8, SC-18
A.10.5 Backup	
A.10.5.1 Information backup	CP-9
A.10.6 Network security management	
A.10.6.1 Network controls	AC-4, AC-17, AC-18, AC-20, CA-3, CP-8, PE-5, SC-7, SC-8, SC-9, SC-10, SC-19, SC-20, SC-21, SC-22, SC-23
A.10.6.2 Security of network services	SA-9, SC-8, SC-9
A.10.7 Media handling	
A.10.7.1 Management of removable media	MP Family, PE-16
A.10.7.2 Disposal of media	MP-6
A.10.7.3 Information handling procedures	MP Family, SI-12
A.10.7.4 Security of system documentation	MP-4, SA-5
A.10.8 Exchange of information	
A.10.8.1 Information exchange policies and procedures	AC-1, AC-3, AC-4, AC-17, AC-18, AC-20, CA-3, PL-4, PS-6, SC-7, SC-16, SI-9
A.10.8.2 Exchange agreements	CA-3, SA-9
A.10.8.3 Physical media in transit	MP-5
A.10.8.4 Electronic messaging	Multiple controls; electronic messaging not addressed separately in SP 800-53
A.10.8.5 Business information systems	CA-1, CA-3
A.10.9 Electronic commerce services	
A.10.9.1 Electronic commerce	AU-10, IA-8, SC-7, SC-8, SC-9, SC-3, SC-14
A.10.9.2 Online transactions	SC-3, SC-7, SC-8, SC-9, SC-14
A.10.9.3 Publicly available information	SC-14
A.10.10 Monitoring	
A.10.10.1 Audit logging	AU-1, AU-2, AU-3, AU-4, AU-5, AU-8, AU-11, AU-12
A.10.10.2 Monitoring system use	AU-1, AU-6, AU-7, PE-6, PE-8, SC-7, SI-4
A.10.10.3 Protection of log information	AU-9
A.10.10.4 Administrator and operator logs	AU-2, AU-12
A.10.10.5 Fault logging	AU-2, AU-6, AU-12, SI-2
A.10.10.6 Clock synchronization	AU-8
A.11 Access Control	
A.11.1 Business requirement for access control	
A.11.1.1 Access control policy	AC-1, AC-5, AC-6, AC-17, AC-18, AC-19, CM-5, MP-1, SI-9
A.11.2 User access management	
A.11.2.1 User registration	AC-1, AC-2, AC-21, IA-5, PE-1, PE-2
A.11.2.2 Privilege management	AC-1, AC-2, AC-6, AC-21, PE-1, PE-2, SI-9
A.11.2.3 User password management	IA-5

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.11.2.4 Review of user access rights	AC-2, PE-2
A 11.3 User responsibilities	
A.11.3.1 Password use	IA-2, IA-5
A.11.3.2 Unattended user equipment	AC-11, IA-2, PE-3, PE-5, PE-18, SC-10
A.11.3.3 Clear desk and clear screen policy	AC-11
A.11.4 Network access control	
A.11.4.1 Policy on use of network services	AC-1, AC-5, AC-6, AC-17, AC-18, AC-20
A.11.4.2 User authentication for external connections	AC-17, AC-18, AC-20, CA-3, IA-2, IA-8
A.11.4.3 Equipment identification in networks	AC-19, IA-3
A.11.4.4 Remote diagnostic and configuration port protection	AC-3, AC-6, AC-17, AC-18, PE-3, MA-3, MA-4
A.11.4.5 Segregation in networks	AC-4, SA-8, SC-7
A.11.4.6 Network connection control	AC-3, AC-6, AC-17, AC-18, SC-7
A.11.4.7 Network routing control	AC-4, AC-17, AC-18
A 11.5 Operating system access control	
A.11.5.1 Secure log-on procedures	AC-7, AC-8, AC-9, AC-10, IA-2, IA-6, IA-8, SC-10
A.11.5.2 User identification and authentication	IA-2, IA-4, IA-5, IA-8
A.11.5.3 Password management system	IA-2, IA-5
A.11.5.4 Use of system utilities	AC-3, AC-6
A.11.5.5 Session time-out	AC-11, SC-10
A.11.5.6 Limitation of connection time	None
A.11.6 Application and information access control	
A.11.6.1 Information access restriction	AC-3, AC-6, AC-14, CM-5
A.11.6.2 Sensitive system isolation	None; SP 800-39
A.11.7 Mobile computing and teleworking	
A.11.7.1 Mobile computing and communications	AC-1, AC-17, AC-18, AC-19, PL-4, PS-6
A.11.7.2 Teleworking	AC-1, AC-4, AC-17, AC-18, PE-17, PL-4, PS-6
A.12 Information systems acquisition, development and maintenance	
A.12.1 Security requirements of information systems	
A.12.1.1 Security requirements analysis and specification	SA-1, SA-3, SA-4
A.12.2 Correct processing in applications	
A.12.2.1 Input data validation	SI-10
A.12.2.2 Control of internal processing	SI-7, SI-9, SI-10
A.12.2.3 Message integrity	AU-10, SC-8, SI-7
A.12.2.4 Output data validation	None
A.12.3 Cryptographic controls	
A.12.3.1 Policy on the use of cryptographic controls	Multiple controls address cryptography (e.g., IA-7, SC-8, SC-9, SC-12, SC-13)
A.12.3.2 Key management	SC-12, SC-17
A.12.4 Security of system files	
A.12.4.1 Control of operational software	CM-1, CM-2, CM-3, CM-4, CM-5, CM-9, PL-4, SA-6, SA-7
A.12.4.2 Protection of system test data	Multiple controls; protection of test data not addressed separately in SP 800-53 (e.g., AC-3, AC-4)
A.12.4.3 Access control to program source code	AC-3, AC-6, CM-5, CM-9, MA-5, SA-10
A.12.5 Security in development and support processes	
A.12.5.1 Change control procedures	CM-1, CM-3, CM-9, SA-10
A.12.5.2 Technical review of applications after operating system changes	CM-3, CM-4, CM-9, SI-2
A.12.5.3 Restrictions on changes to software packages	CM-3, CM-4, CM-5, CM-9
A.12.5.4 Information leakage	AC-4, PE-19
A.12.5.5 Outsourced software development	SA-1, SA-4, SA-6, SA-7, SA-8, SA-9, SA-11, SA-12, SA-13
A.12.6 Technical Vulnerability Management	
A.12.6.1 Control of technical vulnerabilities	RA-3, RA-5, SI-2, SI-5
A.13 Information security incident management	
A.13.1 Reporting information security events and weaknesses	
A.13.1.1 Reporting information security events	AU-6, IR-1, IR-6, SI-4, SI-5

ISO/IEC 27001 (Annex A) CONTROLS	NIST SP 800-53 CONTROLS
A.13.1.2 Reporting security weaknesses	PL-4, SI-2, SI-4, SI-5
A.13.2 Management of information security incidents and improvements	
A.13.2.1 Responsibilities and procedures	IR-1
A.13.2.2 Learning from information security incidents	IR-4
A.13.2.3 Collection of evidence	AU-9, IR-4
A.14 Business continuity management	
A.14.1 Information security aspects of business continuity management	
A.14.1.1 Including information security in the business continuity management process	CP-1, CP-2, CP-4
A.14.1.2 Business continuity and risk assessment	CP-2, PM-9, RA Family
A.14.1.3 Developing and implementing continuity plans including information security	CP Family
A.14.1.4 Business continuity planning framework	CP-2, CP-4
A.14.1.5 Testing, maintaining and reassessing business continuity plans	CP-2, CP-4
A.15 Compliance	
A.15.1 Compliance with legal requirements	
A.15.1.1 Identification of applicable legislation	XX-1 controls, IA-7
A.15.1.2 Intellectual property rights (IPR)	SA-6
A.15.1.3 Protection of organizational records	AU-9, AU-11, CP-9, MP-1, MP-4, SA-5, SI-12
A.15.1.4 Data protection and privacy of personal information	PL-5; SI-12
A.15.1.5 Prevention of misuse of information processing facilities	AC-8, AU-6, PL-4, PS-6, PS-8, SA-7
A.15.1.6 Regulation of cryptographic controls	IA-7, SC-13
A.15.2 Compliance with security policies and standards, and technical compliance	
A.15.2.1 Compliance with security policies and standards	XX-1 controls, AC-2, CA-2, CA-7, IA-7, PE-8, SI-12
A.15.2.2 Technical compliance checking	CA-2, CA-7, RA-5
A.15.3 Information systems audit considerations	
A.15.3.1 Information systems audit controls	AU-1, AU-2, PL-6
A.15.3.2 Protection of information systems audit tools	AU-9

APPENDIX I

INDUSTRIAL CONTROL SYSTEMS

SECURITY CONTROLS, ENHANCEMENTS, AND SUPPLEMENTAL GUIDANCE

Industrial control systems (ICS)[78] are information systems that differ significantly from traditional administrative, mission support, and scientific data processing information systems. ICS typically have many unique characteristics—including a need for real-time response and extremely high availability, predictability, and reliability. These types of specialized systems are pervasive throughout the critical infrastructure, often being required to meet several and often conflicting safety, operational, performance, reliability, and security requirements such as: (i) minimizing risk to the health and safety of the public; (ii) preventing serious damage to the environment; (iii) preventing serious production stoppages or slowdowns that result in negative impact to the Nation's economy and ability to carry out critical functions; (iv) protecting the critical infrastructure from cyber attacks and common human error; and (v) safeguarding against the compromise of proprietary information.[79]

Previously, ICS had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated more closely into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, portions of these ICS have started to resemble the more traditional information systems. Increasingly, ICS use the same commercially available hardware and software components as are used in the organization's traditional information systems. While the change in ICS architecture supports new information system capabilities, it also provides significantly less isolation from the outside world for these systems, introducing many of the same vulnerabilities that exist in current networked information systems. The result is an even greater need to secure ICS.

FIPS 200, supported by NIST Special Publication 800-53, requires that federal agencies (and organizations subordinate to those agencies) implement minimum security controls for their organizational information systems based on the FIPS 199 security categorization of those systems. This includes implementing the baseline security controls described in this document in ICS that are operated by or on behalf of federal agencies. Section 3.3, *Tailoring the Initial Baseline*, allows organizations[80] to modify or adjust recommended security control baselines when certain conditions exist that require that flexibility. NIST recommends that ICS owners take advantage of the ability to tailor the initial baselines applying the ICS-specific guidance in this appendix. This appendix also contains additions to the initial security control baselines that have been determined to be generally required for ICS.

[78] An ICS is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC). ICS are typically found in the electric, water, oil and gas, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (automotive, aerospace, and durable goods) industries as well as in air and rail transportation control systems.

[79] See Executive Order 13231 on Critical Infrastructure Protection, October 16, 2001.

[80] NIST Special Publication 800-53 employs the term *organization* to refer to the owner or operator of an information system. In this Appendix, organization may refer to the owner or operator of an ICS.

NIST has worked cooperatively with ICS communities in the public and private sectors to develop specific guidance on the application of the security controls in this document to ICS. That guidance, contained in this Appendix, includes ICS-specific:

- Tailoring guidance;
- Supplements to the security control baselines; and
- Supplemental guidance.

ICS Tailoring Guidance

Tailoring guidance for ICS can include scoping guidance and the application of compensating security controls. Due to the unique characteristics of ICS, these systems may require a greater use of compensating security controls than is the case for general-purpose information systems.

Implementation Tip

In situations where the ICS cannot support, or the organization determines it is not advisable to implement particular security controls or control enhancements in an ICS (e.g., performance, safety, or reliability are adversely impacted), the organization provides a complete and convincing rationale for how the selected compensating controls provide an equivalent security capability or level of protection for the ICS and why the related baseline security controls could not be employed.

In accordance with the Technology-related Considerations of the Scoping Guidance in Section 3.3, if automated mechanisms are not readily available, cost-effective, or technically feasible in the ICS, compensating security controls, implemented through nonautomated mechanisms or procedures are employed.

Compensating controls are not exceptions or waivers to the baseline controls; rather, they are alternative safeguards and countermeasures employed within the ICS that accomplish the intent of the original security controls that could not be effectively employed. Organizational decisions on the use of compensating controls are documented in the security plan for the ICS.

The security controls and control enhancements listed in Table I-1 are likely candidates for tailoring with the applicability of scoping guidance indicated for each control/enhancement. In Table I-1, the citation of a control without enhancements (e.g., AC-17) refers only to the base control without any enhancements, while reference to an enhancement by a parenthetical number following the control identification (e.g., AC-17(1)) refers only to the specific control enhancement.

TABLE I-1: SECURITY CONTROL CANDIDATES FOR TAILORING

CONTROL NUMBER	CONTROL NAME	TAILORING OPTIONS	
		SCOPING GUIDANCE	COMPENSATING CONTROLS
AC-2	Account Management	NO	YES
AC-5	Separation of Duties	NO	YES
AC-6	Least Privilege	NO	YES
AC-7	Unsuccessful Login Attempts	NO	YES
AC-8	System Use Notification	NO	YES
AC-10	Concurrent Session Control	NO	YES
AC-11	Session Lock	NO	YES
AC-17	Remote Access	NO	YES
AC-17 (2)	Remote Access	NO	YES
AC-18 (1)	Wireless Access	NO	YES
AC-19	Access Control for Mobile Devices	NO	YES
AU-2	Auditable Events	NO	YES
AU-5	Response to Audit Processing Failure	YES	YES
AU-7	Audit Reduction and Report Generation	YES	YES
AU-12	Audit Generation	NO	YES
AU-12 (1)	Audit Generation	NO	YES
CA-2	Security Assessments	NO	YES
CP-4	Contingency Plan Testing and Exercises	NO	YES
CP-4 (1)	Contingency Plan Testing and Exercises	NO	YES
CP-4 (2)	Contingency Plan Testing and Exercises	NO	YES
CP-4 (4)	Contingency Plan Testing and Exercises	NO	YES
CP-7	Alternate Processing Site	NO	YES
IA-2	User Identification and Authentication (Organizational Users)	NO	YES
IA-3	Device Identification and Authentication	NO	YES
MA-4 (3)	Non-Local Maintenance	YES	YES
MP-5 (4)	Media Transport	YES	YES
PE-6 (2)	Monitoring Physical Access	YES	YES
RA-5	Vulnerability Scanning	NO	YES
SC-2	Application Partitioning	YES	YES
SC-3	Security Function Isolation	NO	YES
SC-7 (6)	Boundary Protection	YES	NO
SC-7 (8)	Boundary Protection	YES	YES
SC-10	Network Disconnect	NO	YES
SI-2 (1)	Flaw Remediation	YES	YES
SI-3 (1)	Malicious Code Protection	YES	YES
SI-8 (1)	Spam Protection	YES	YES

ICS Supplements to the Security Control Baselines

The following table lists the recommended ICS supplements (highlighted in **bold** text) to the security control baselines in Appendix D.

TABLE I-2: ICS SUPPLEMENTS TO SECURITY CONTROL BASELINES

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-3	Access Enforcement	AC-3	AC-3 **(2)**	AC-3 **(2)**
Physical and Environmental Protection				
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9 **(1)**	PE-9 **(1)**
PE-11	Emergency Power	**PE-11**	PE-11 **(1)**	PE-11 (1) **(2)**
System and Communications Protection				
SC-24	Fail in Known State	Not Selected	**SC-24**	SC-24
System and Information Integrity				
SI-13	Predictable Failure Prevention	Not Selected	Not Selected	**SI-13**

In addition to the security controls added for ICS in the table above, the security control supplement process described in Section 3.4 is still applicable to ICS. Organizations are required to conduct a risk assessment taking into account the tailoring and supplementing performed in arriving at the agreed-upon set of security controls for the ICS and the risk to the organization's operations and assets, individuals, other organizations, and the Nation being incurred by operation of the ICS with the intended controls. The organization decides whether that risk is acceptable, and if not, supplements the control set with additional controls until an acceptable level of risk is obtained.

ICS Supplemental Guidance

ICS Supplemental Guidance provides organizations with additional information on the application of the security controls and control enhancements in Appendix F to ICS and the environments in which these specialized systems operate. The Supplemental Guidance also provides information as to why a particular security control or control enhancement may not be applicable in some ICS environments and may be a candidate for tailoring (i.e., the application of scoping guidance and/or compensating controls). ICS Supplemental Guidance does not replace the original Supplemental Guidance in Appendix F.

ACCESS CONTROL

AC-2 ACCOUNT MANAGEMENT

ICS Supplemental Guidance: In situations where physical access to the ICS (e.g., workstations, hardware components, field devices) predefines account privileges or where the ICS (e.g., certain remote terminal units, meters, relays) cannot support account management, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, intrusion detection, auditing measures) in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS (e.g., field devices) cannot support the use of automated mechanisms for the management of information system accounts, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-3 ACCESS ENFORCEMENT

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

References: NIST Special Publication 800-82.

AC-5 SEPARATION OF DUTIES

ICS Supplemental Guidance: In situations where the ICS cannot support the differentiation of roles, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing) in accordance with the general tailoring guidance. The organization carefully considers the appropriateness of a single individual performing multiple critical roles.

AC-6 LEAST PRIVILEGE

ICS Supplemental Guidance: In situations where the ICS cannot support differentiation of privileges, the organization employs appropriate compensating controls (e.g., providing increased personnel security and auditing) in accordance with the general tailoring guidance. The organization carefully considers the appropriateness of a single individual having multiple critical privileges.

AC-7 UNSUCCESSFUL LOGIN ATTEMPTS

ICS Supplemental Guidance: In situations where the ICS cannot support account/node locking or delayed login attempts, or the ICS cannot perform account/node locking or delayed logins due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., logging or recording all unsuccessful login attempts and alerting ICS security personnel though alarms or other means when the number of organization-defined consecutive invalid access attempts is exceeded) in accordance with the general tailoring guidance.

AC-8 SYSTEM USE NOTIFICATION

ICS Supplemental Guidance: In situations where the ICS cannot support system use notification, the organization employs appropriate compensating controls (e.g., posting physical notices in ICS facilities) in accordance with the general tailoring guidance.

AC-10 CONCURRENT SESSION CONTROL

ICS Supplemental Guidance: In situations where the ICS cannot support concurrent session control, the organization employs appropriate compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

AC-11 SESSION LOCK

ICS Supplemental Guidance: The ICS employs session lock to prevent access to specified workstations/nodes. The ICS activates session lock mechanisms automatically after an organization-defined time period for designated workstations/nodes on the ICS. In some cases, session lock for ICS operator workstations/nodes is not advised (e.g., when immediate operator responses are required in emergency situations). Session lock is not a substitute for logging out of the ICS. In situations where the ICS cannot support session lock, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

AC-17 REMOTE ACCESS

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms for monitoring and control of remote access methods, the organization employs nonautomated mechanisms or procedures as compensating controls (e.g., following manual authentication [see IA-2 in this appendix], dial-in remote access may be enabled for a specified period of time or a call may be placed from the ICS site to the authenticated remote entity) in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic mechanism (e.g., encryption, digital signature, hash function). Each mechanism has a different delay impact. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of remote sessions, or the components cannot use cryptographic mechanisms due to significant adverse impact on safety, performance, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing for remote sessions or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

AC-18 WIRELESS ACCESS

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity, and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic mechanism (e.g., encryption, digital signature, hash function). Each mechanism has a different delay impact. In situations where the ICS cannot support the use of cryptographic mechanisms to protect the confidentiality and integrity of wireless access, or the components cannot use cryptographic mechanisms due to significant adverse impact on safety, performance, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing for wireless access or limiting wireless access privileges to key personnel) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

AC-19 ACCESS CONTROL FOR MOBILE DEVICES

ICS Supplemental Guidance: In situations where the ICS cannot implement any or all of the components of this control, the organization employs other mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

AC-22 PUBLICLY ACCESSIBLE CONTENT

ICS Supplemental Guidance: Generally, public access to ICS information is not permitted.

AWARENESS AND TRAINING

AT-2 SECURITY AWARENESS

ICS Supplemental Guidance: Security awareness training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security awareness program is consistent with the requirements of the security awareness and training policy established by the organization.

AT-3 SECURITY TRAINING

ICS Supplemental Guidance: Security training includes initial and periodic review of ICS-specific policies, standard operating procedures, security trends, and vulnerabilities. The ICS security training program is consistent with the requirements of the security awareness and training policy established by the organization.

AUDITING AND ACCOUNTABILITY

AU-2 AUDITABLE EVENTS

ICS Supplemental Guidance: Most ICS auditing occurs at the application level.

AU-5 RESPONSE TO AUDIT PROCESSING FAILURES

ICS Supplemental Guidance: In general, audit record processing is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing, including response to audit failures, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

AU-7 AUDIT REDUCTION AND REPORT GENERATION

ICS Supplemental Guidance: In general, audit reduction and report generation is not performed on the ICS, but on a separate information system. In situations where the ICS cannot support auditing including audit reduction and report generation, the organization employs compensating controls (e.g., providing an auditing capability on a separate information system) in accordance with the general tailoring guidance.

AU-12 AUDIT GENERATION

ICS Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to generate audit records, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SECURITY ASSESSMENT AND AUTHORIZATION

CA-2 SECURITY ASSESSMENTS

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before an assessment can be conducted. If an ICS must be taken off-line to conduct an assessment, the assessment is scheduled to occur during planned ICS outages whenever possible. In situations where the organization cannot, for operational reasons, conduct a live assessment of a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct the assessment) in accordance with the general tailoring guidance.

CA-7 CONTINUOUS MONITORING

ICS Supplemental Guidance: Assessments are performed and documented by qualified assessors (i.e., experienced in assessing ICS) authorized by the organization. The organization ensures that assessments do not interfere with ICS functions. The individual/group conducting the assessment fully understands the organizational information security policies and procedures, the ICS security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. Ongoing assessments of ICS may not be feasible. See CA-2 ICS Supplemental Guidance in this appendix.

CONFIGURATION MANAGEMENT

CM-3 CONFIGURATION CHANGE CONTROL

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to implement configuration change control, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-4 SECURITY IMPACT ANALYSIS

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.

CM-5 ACCESS RESTRICTIONS FOR CHANGE

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to enforce access restrictions and support auditing of enforcement actions, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot prevent the installation of software programs that are not signed with an organizationally-recognized and approved certificate, the organization employs alternative mechanisms or procedures as compensating controls (e.g., auditing of software installation) in accordance with the general tailoring guidance.

CM-6 CONFIGURATION SETTINGS

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to centrally manage, apply, and verify configuration settings, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

CM-7 LEAST FUNCTIONALITY

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot employ automated mechanisms to prevent program execution, the organization employs compensating controls (e.g., external automated mechanisms, procedures) in accordance with the general tailoring guidance.

CONTINGENCY PLANNING

CP-2 CONTINGENCY PLAN

ICS Supplemental Guidance: The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the ICS executes predetermined procedures (e.g., alert the operator of the failure and then do nothing, alert the operator and then safely shut down the industrial process, alert the operator and then maintain the last operational setting prior to failure). Consideration is given to restoring system state variables as part of restoration (e.g., valves are restored to their original settings prior to the disruption).

References: NIST Special Publication 800-82.

CP-4 CONTINGENCY PLAN TESTING AND EXERCISES

ICS Supplemental Guidance: In situations where the organization cannot test or exercise the contingency plan on production ICS due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., using scheduled and unscheduled system maintenance activities including responding to ICS component and system failures, as an opportunity to test or exercise the contingency plan) in accordance with the general tailoring guidance.

CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

ICS Supplemental Guidance: Reconstitution of the ICS includes restoration of system state variables (e.g., valves are restored to their appropriate settings as part of the reconstitution).

IDENTIFICATION AND AUTHENTICATION

IA-2 USER IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification and authentication may be role-based, group-based, or device-based. For certain ICS, the capability for immediate operator interaction is critical. Local emergency actions for ICS are not hampered by identification or authentication requirements. Access to these systems may be restricted by appropriate physical security controls. In situations where the ICS cannot support user identification and authentication, or the organization determines it is not advisable to perform user identification and authentication due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased physical security, personnel security, and auditing measures) in accordance with the general tailoring guidance. For example, manual voice authentication of remote personnel and local, manual actions may be required in order to establish a remote access. See AC-17 ICS Supplemental Guidance in this appendix. Local user access to ICS components is enabled only when necessary, approved, and authenticated.

Control Enhancements: (1) (2) (3)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support multifactor authentication, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

ICS Supplemental Guidance: In situations where the ICS cannot support device identification and authentication (e.g., serial devices), the organization employs compensating controls (e.g., implementing physical security measures) in accordance with the general tailoring guidance.

IA-4 IDENTIFIER MANAGEMENT

ICS Supplemental Guidance: Where users function as a single group (e.g., control room operators), user identification may be role-based, group-based, or device-based.

References: NIST Special Publication 800-82.

IA-5 AUTHENTICATOR MANAGEMENT

References: NIST Special Publication 800-82.

IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION

ICS Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

INCIDENT RESPONSE

IR-6 INCIDENT REPORTING

ICS Supplemental Guidance: The United States Computer Emergency Readiness Team (US-CERT) maintains the ICS Security Center at http://www.uscert.gov/control_systems.

References: NIST Special Publication 800-82.

MAINTENANCE

MA-4 NON-LOCAL MAINTENANCE

Control Enhancement: (3)

ICS Enhancement Supplemental Guidance: In crisis or emergency situations, the organization may need immediate access to non-local maintenance and diagnostic services in order to restore essential ICS operations or services. In situations where the organization may not have access to non-local maintenance or diagnostic service at the required level of security, the organization employs appropriate compensating controls (e.g., limiting the extent of the maintenance and diagnostic services to the minimum essential activities, carefully monitoring and auditing the non-local maintenance and diagnostic activities) in accordance with the general tailoring guidance.

MEDIA PROTECTION

MP-5 MEDIA TRANSPORT

Control Enhancement: (4)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support cryptographic mechanisms, the organization employs compensating controls in accordance with the general tailoring guidance (e.g., implementing physical security measures).

PHYSICAL AND ENVIRONMENTAL PROTECTION

PE-3 PHYSICAL ACCESS CONTROL

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies. The organization considers access requirements in emergency situations. During an emergency-related event, the organization may restrict access to ICS facilities and assets to authorized individuals only. ICS are often constructed of devices that either do not have or cannot use comprehensive access control capabilities due to time-restrictive safety constraints. Physical access controls and defense-in-depth measures are used by the organization when necessary and possible to supplement ICS security when electronic mechanisms are unable to fulfill the security requirements of the organization's security plan.

References: NIST Special Publication 800-82.

PLANNING

PL-2 SYSTEM SECURITY PLAN

References: NIST Special Publication 800-82.

RISK ASSESSMENT

RA-2 SECURITY CATEGORIZATION

References: NIST Special Publication 800-82.

RA-3 RISK ASSESSMENT

References: NIST Special Publication 800-82.

RA-5 VULNERABILITY SCANNING

ICS Supplemental Guidance: Vulnerability scanning and penetration testing are used with care on ICS networks to ensure that ICS functions are not adversely impacted by the scanning process. Production ICS may need to be taken off-line, or replicated to the extent feasible, before scanning can be conducted. If ICS are taken off-line for scanning, scans are scheduled to occur during planned ICS outages whenever possible. If vulnerability scanning tools are used on non-ICS networks, extra care is taken to ensure that they do not scan the ICS network. In situations where the organization cannot, for operational reasons, conduct vulnerability scanning on a production ICS, the organization employs compensating controls (e.g., providing a replicated system to conduct scanning) in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

SYSTEM AND SERVICES ACQUISITION

SA-4 ACQUISITIONS

ICS Supplemental Guidance: The SCADA/Control Systems Procurement Project provides example cyber security procurement language for ICS.

References: Web: WWW.MSISAC.ORG/SCADA.

SA-8 SECURITY ENGINEERING PRINCIPLES

References: NIST Special Publication 800-82.

SYSTEM AND COMMUNICATIONS PROTECTION

SC-2 APPLICATION PARTITIONING

ICS Supplemental Guidance: In situations where the ICS cannot separate user functionality from information system management functionality, the organization employs compensating controls (e.g., providing increased auditing measures) in accordance with the general tailoring guidance.

SC-3 SECURITY FUNCTION ISOLATION

ICS Supplemental Guidance: In situations where the ICS cannot support security function isolation, the organization employs compensating controls (e.g., providing increased auditing measures, limiting network connectivity) in accordance with the general tailoring guidance.

SC-7 BOUNDARY PROTECTION

Control Enhancements: (1) (2)

ICS Enhancement Supplemental Guidance: Generally, public access to ICS information is not permitted.

Control Enhancement: (6)

ICS Enhancement Supplemental Guidance: The organization selects an appropriate failure mode (e.g., fail closed, fail open).

SC-8 TRANSMISSION INTEGRITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The organization explores all possible cryptographic integrity mechanisms (e.g., digital signature, hash function). Each mechanism has a different delay impact.

SC-9 TRANSMISSION CONFIDENTIALITY

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: ICS security objectives typically follow the priority of availability, integrity and confidentiality, in that order. The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-10 NETWORK DISCONNECT

ICS Supplemental Guidance: In situations where the ICS cannot terminate a network connection at the end of a session or after an organization-defined time period of inactivity, or the ICS cannot terminate a network connection due to significant adverse impact on performance, safety, or reliability, the organization employs appropriate compensating controls (e.g., providing increased auditing measures or limiting remote access privileges to key personnel) in accordance with the general tailoring guidance.

SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

ICS Supplemental Guidance: The use of cryptography, including key management, is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS. The use of cryptographic key management in ICS is intended to support internal nonpublic use.

SC-13 USE OF CRYPTOGRAPHY

ICS Supplemental Guidance: The use of cryptography is determined after careful consideration of the security needs and the potential ramifications on system performance. For example, the organization considers whether latency induced from the use of cryptography would adversely impact the operational performance of the ICS.

SC-14 PUBLIC ACCESS PROTECTIONS

ICS Supplemental Guidance: Generally, public access to ICS is not permitted.

SC-15 COLLABORATIVE COMPUTING DEVICES

ICS Supplemental Guidance: Generally, collaborative computing mechanisms are not permitted on ICS.

SC-19 VOICE OVER INTERNET PROTOCOL

ICS Supplemental Guidance: The use of VoIP technologies is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-21 SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-22 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

ICS Supplemental Guidance: The use of secure name/address resolution services is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

SC-23 SESSION AUTHENTICITY

ICS Supplemental Guidance: In situations where the ICS cannot protect the authenticity of communications sessions, the organization employs compensating controls (e.g., auditing measures) in accordance with the general tailoring guidance.

SYSTEM AND INFORMATION INTEGRITY

SI-2 FLAW REMEDIATION

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage flaw remediation and automatic updates, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to conduct and report on the status of flaw remediation, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

SI-3 MALICIOUS CODE PROTECTION

ICS Supplemental Guidance: The use of malicious code protection is determined after careful consideration and after verification that it does not adversely impact the operational performance of the ICS.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage malicious code protection mechanisms, the organization employs appropriate compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated mechanisms to update malicious code protection mechanisms, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

References: NIST Special Publication 800-82.

SI-4 INFORMATION SYSTEM MONITORING

ICS Supplemental Guidance: The organization ensures that the use of monitoring tools and techniques does not adversely impact the operational performance of the ICS.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot support the use of automated tools to support near-real-time analysis of events, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

Control Enhancement: (6)

ICS Enhancement Supplemental Guidance: In situations where the ICS cannot prevent non-privileged users from circumventing intrusion detection and prevention capabilities, the organization employs appropriate compensating controls (e.g., enhanced auditing) in accordance with the general tailoring guidance.

SI-6 SECURITY FUNCTIONALITY VERIFICATION

ICS Supplemental Guidance: Generally, it is not recommended to shut down and restart the ICS upon the identification of an anomaly.

SI-7 SOFTWARE AND INFORMATION INTEGRITY

ICS Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

Control Enhancements: (1)

ICS Enhancement Supplemental Guidance: The organization ensures that the use of integrity verification applications does not adversely impact the operational performance of the ICS.

Control Enhancement: (2)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot employ automated tools that provide notification of integrity discrepancies, the organization employs nonautomated mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

SI-8 SPAM PROTECTION

ICS Supplemental Guidance: The organization removes unused and unnecessary functions and services (e.g., electronic mail, Internet access). Due to differing operational characteristics between ICS and general purpose information systems, ICS do not generally employ spam protection mechanisms. Unusual traffic flow (e.g., during crisis situations), may be misinterpreted and detected as spam, which can cause issues with the ICS and possible system failure.

Control Enhancement: (1)

ICS Enhancement Supplemental Guidance: In situations where the organization cannot centrally manage spam protection mechanisms, the organization employs local mechanisms or procedures as compensating controls in accordance with the general tailoring guidance.

National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

NIST Special Publication 800-122

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

Recommendations of the National Institute of Standards and Technology

Erika McCallister
Tim Grance
Karen Scarfone

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

April 2010

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation’s measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL’s responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL’s research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-122
Natl. Inst. Stand. Technol. Spec. Publ. 800-122, 59 pages (Apr. 2010)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgments

The authors, Erika McCallister, Tim Grance, and Karen Scarfone of the National Institute of Standards and Technology (NIST), wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. Of particular note are the efforts of Joseph Nusbaum of Innovative Analytics & Training, Deanna DiCarlantonio of CUNA Mutual Group, and Michael L. Shapiro and Daniel I. Steinberg of Booz Allen Hamilton, who contributed significant portions to previous versions of the document. The authors would also like to acknowledge Ron Ross, Kelley Dempsey, and Arnold Johnson of NIST; Michael Gerdes, Beth Mallory, and Victoria Thompson of Booz Allen Hamilton; Brendan Van Alsenoy of ICRI, K.U.Leuven; David Plocher and John de Ferrari of the Government Accountability Office; Toby Levin of the Department of Homeland Security; Idris Adjerid of Carnegie Mellon University; The Federal Committee on Statistical Methodology: Confidentiality and Data Access Committee; The Privacy Best Practices Subcommittee of the Chief Information Officers Council; and Julie McEwen and Aaron Powell of The MITRE Corporation, for their keen and insightful assistance during the development of the document.

Table of Contents

Appendices

Executive Summary

The escalation of security breaches involving personally identifiable information (PII) has contributed to the loss of millions of records over the past few years.[1] Breaches involving PII are hazardous to both individuals and organizations. Individual harms[2] may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or remediation costs. To appropriately protect the confidentiality of PII, organizations should use a risk-based approach; as McGeorge Bundy[3] once stated, "If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds." This document provides guidelines for a risk-based approach to protecting the confidentiality[4] of PII. The recommendations in this document are intended primarily for U.S. Federal government agencies and those who conduct business on behalf of the agencies,[5] but other organizations may find portions of the publication useful. Each organization may be subject to a different combination of laws, regulations, and other mandates related to protecting PII, so an organization's legal counsel and privacy officer should be consulted to determine the current obligations for PII protection. For example, the Office of Management and Budget (OMB) has issued several memoranda with requirements for how Federal agencies must handle and protect PII. To effectively protect PII, organizations should implement the following recommendations.

Organizations should identify all PII residing in their environment.

An organization cannot properly protect PII it does not know about. This document uses a broad definition of PII to identify as many potential sources of PII as possible (e.g., databases, shared network drives, backup tapes, contractor sites). PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[6] Examples of PII include, but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)

[1] Government Accountability Office (GAO) Report 08-343, *Protecting Personally Identifiable Information*, January 2008, http://www.gao.gov/new.items/d08343.pdf

[2] For the purposes of this document, *harm* means any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. See Section 3.1 for additional information.

[3] Congressional testimony as quoted by the New York Times, March 5, 1989. McGeorge Bundy was the U.S. National Security Advisor to Presidents Kennedy and Johnson (1961-1966). http://query.nytimes.com/gst/fullpage.html?res=950DE2D6123AF936A35750C0A96F948260

[4] For the purposes of this document, confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information." 44 U.S.C. § 3542. http://uscode.house.gov/download/pls/44C35.txt.

[5] For the purposes of this publication, both are referred to as "organizations".

[6] This definition is the GAO expression of an amalgam of the definitions of PII from OMB Memorandums 07-16 and 06-19. GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008, http://www.gao.gov/new.items/d08536.pdf.

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

The likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores. For example, an organization should only request PII in a new form if the PII is absolutely necessary. Also, an organization should regularly review its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission. For example, organizations could have an annual PII purging awareness day.[7]

OMB M-07-16[8] specifically requires agencies to:

- Review current holdings of PII and ensure they are accurate, relevant, timely, and complete
- Reduce PII holdings to the minimum necessary for proper performance of agency functions
- Develop a schedule for periodic review of PII holdings
- Establish a plan to eliminate the unnecessary collection and use of SSNs.

Organizations should categorize their PII by the PII confidentiality impact level.

All PII is not created equal. PII should be evaluated to determine its PII confidentiality impact level, which is different from the Federal Information Processing Standard (FIPS) Publication 199[9] confidentiality impact level, so that appropriate safeguards can be applied to the PII. The PII confidentiality impact level—*low, moderate, or high*—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. This document provides a list of factors an organization should consider when determining the PII confidentiality impact level. Each organization should decide which factors it will use for determining impact levels and then create and implement the appropriate policy, procedures, and controls. The following are examples of factors:

- **Identifiability.** Organizations should evaluate how easily PII can be used to identify specific individuals. For example, a SSN uniquely and directly identifies an individual, whereas a telephone area code identifies a set of people.
- **Quantity of PII.** Organizations should consider how many individuals can be identified from the PII. Breaches of 25 records and 25 million records may have different impacts. The PII confidentiality impact level should only be raised and not lowered based on this factor.
- **Data Field Sensitivity.** Organizations should evaluate the sensitivity of each individual PII data field. For example, an individual's SSN or financial account number is generally more sensitive than

[7] Disposal of PII should be conducted in accordance with the retention schedules approved by the National Archives and Records Administration (NARA), as well as in accordance with agency litigation holds.

[8] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

[9] FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

an individual's phone number or ZIP code. Organizations should also evaluate the sensitivity of the PII data fields when combined.

- **Context of Use.** Organizations should evaluate the context of use—the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated. The context of use may cause the same PII data elements to be assigned different PII confidentiality impact levels based on their use. For example, suppose that an organization has two lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization, and the second list is people who work undercover in law enforcement. If the confidentiality of the lists is breached, the potential impacts to the affected individuals and to the organization are significantly different for each list.

- **Obligations to Protect Confidentiality.** An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Obligations to protect generally include laws, regulations, or other mandates (e.g., Privacy Act, OMB guidance). For example, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to specific legal obligations to protect certain types of PII.[10]

- **Access to and Location of PII.** Organizations may choose to take into consideration the nature of authorized access to and the location of PII. When PII is accessed more often or by more people and systems, or the PII is regularly transmitted or transported offsite, then there are more opportunities to compromise the confidentiality of the PII.

Organizations should apply the appropriate safeguards for PII based on the PII confidentiality impact level.

Not all PII should be protected in the same way. Organizations should apply appropriate safeguards to protect the confidentiality of PII based on the PII confidentiality impact level. Some PII does not need to have its confidentiality protected, such as information that the organization has permission or authority to release publicly (e.g., an organization's public phone directory). NIST recommends using operational safeguards, privacy-specific safeguards, and security controls,[11] such as:

- **Creating Policies and Procedures.** Organizations should develop comprehensive policies and procedures for protecting the confidentiality of PII.

- **Conducting Training.** Organizations should reduce the possibility that PII will be accessed, used, or disclosed inappropriately by requiring that all individuals receive appropriate training before being granted access to systems containing PII.

- **De-Identifying PII.** Organizations can de-identify records by removing enough PII such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. De-identified records can be used when full records are not necessary, such as for examinations of correlations and trends.

- **Using Access Enforcement.** Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists).

- **Implementing Access Control for Mobile Devices.** Organizations can prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital

[10] The Census Bureau has a special obligation to protect based on provisions of Title 13 of the U.S. Code, and IRS has a special obligation to protect based on Title 26 of the U.S. Code. There are more agency-specific obligations to protect PII, and an organization's legal counsel and privacy officer should be consulted.

[11] This document provides some selected security control examples from NIST SP 800-53.

assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).

- **Providing Transmission Confidentiality.** Organizations can protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted.
- **Auditing Events.** Organizations can monitor events that affect the confidentiality of PII, such as inappropriate access to PII.

Organizations should develop an incident response plan to handle breaches involving PII.

Breaches involving PII are hazardous to both individuals and organizations. Harm to individuals and organizations can be contained and minimized through the development of effective incident response plans for breaches involving PII. Organizations should develop plans[12] that include elements such as determining when and how individuals should be notified, how a breach should be reported, and whether to provide remedial services, such as credit monitoring, to affected individuals.

Organizations should encourage close coordination among their chief privacy officers, senior agency officials for privacy, chief information officers, chief information security officers, and legal counsel[13] when addressing issues related to PII.

Protecting the confidentiality of PII requires knowledge of information systems, information security, privacy, and legal requirements. Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time. Additionally, new policies often require the implementation of technical security controls to enforce the policies. Close coordination of the relevant experts helps to prevent incidents that could result in the compromise and misuse of PII by ensuring proper interpretation and implementation of requirements.

[12] OMB requires agencies to develop and implement breach notification policies. OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf.

[13] Some organizations are structured differently and have different names for roles. These roles are examples, used for illustrative purposes.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), “Securing Agency Information Systems,” as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies, also referred to as organizations in the guide. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

The purpose of this document is to assist Federal agencies in protecting the confidentiality of personally identifiable information (PII) in information systems. The document explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy using the Fair Information Practices, which are the principles underlying most privacy laws and privacy best practices. PII should be protected from inappropriate access, use, and disclosure. This document provides practical, context-based guidance for identifying PII and determining what level of protection is appropriate for each instance of PII. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII. Organizations are encouraged to tailor the recommendations to meet their specific requirements.

1.3 Audience

The primary audience for this document is the individuals who apply policies and procedures for protecting the confidentiality of PII on Federal information systems, as well as technical and non-technical personnel involved with implementing system-level changes concerning PII protection methods. Individuals in many roles should find this document useful, including chief privacy officers and other privacy officers, privacy advocates, privacy support staff, public affairs staff, compliance officers, human resources staff, system administrators, chief information security officers, information system security officers, information security support staff, computer security incident response teams, and chief information officers.

1.4 Document Structure

The remainder of this document is organized into the following sections:

- Section 2 provides an introduction to PII and the Fair Information Practices, and it explains how to locate PII maintained by an organization.
- Section 3 describes factors for determining the potential impact of inappropriate access, use, and disclosure of PII.
- Section 4 presents several methods for protecting the confidentiality of PII that can be implemented to reduce PII exposure and risk.
- Section 5 provides recommendations for developing an incident response plan for breaches involving PII and integrating the plan into an organization's existing incident response plan.

The following appendices are also included for additional information:

- Appendix A provides samples of PII-related scenarios and questions that can be adapted for an organization's training exercises.
- Appendix B presents frequently asked questions (FAQ) related to protecting the confidentiality of PII.
- Appendix C contains other terms and definitions for personal information.
- Appendix D provides additional information about the Fair Information Practices that may be helpful in understanding the framework underlying most privacy laws.
- Appendix E provides a glossary of selected terms from the publication.
- Appendix F contains a list of acronyms and abbreviations used within the publication.
- Appendix G presents a list of resources that may be helpful for gaining a better understanding of PII, PII protection, and related topics.

2. Introduction to PII

One of the most widely used terms to describe personal information is PII. Examples of PII range from an individual's name or email address to an individual's financial and medical records or criminal history. Unauthorized access, use, or disclosure of PII can seriously harm both individuals, by contributing to identity theft, blackmail, or embarrassment, and the organization, by reducing public trust in the organization or creating legal liability. This section explains how to identify and locate PII[14] maintained within an organization's environment and/or under its control, and it provides an introduction to the Fair Information Practices. Sections 3 and 4 discuss factors for assigning PII impact levels and selecting safeguards, respectively. Section 5 discusses incident response for breaches involving PII.

2.1 Identifying PII

PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[15]

To *distinguish* an individual[16] is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data.[17] In contrast, a list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.[18]

To *trace* an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status. For example, an audit log containing records of user actions could be used to trace an individual's activities.

Linked information is information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.

[14] Even if an organization determines that information is not PII, the organization should still consider whether the information is sensitive or has organizational or individual risks associated with it and determine the appropriate protections.

[15] GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008, http://www.gao.gov/new.items/d08536.pdf.

[16] The terms "individual" and "individual's identity" are used interchangeably throughout this document. For additional information about the term *individual*, see Appendix B.

[17] These data elements are included in a list of identifying information from the Identity Theft and Assumption Deterrence Act of 1998, Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998).

[18] Information elements that are not sufficient to identify an individual when considered separately might nevertheless render the individual identifiable when combined with additional information. For instance, if the list of credit scores were to be supplemented with information, such as age, address, and gender, it is probable that this additional information would render the individuals identifiable.

Organizations are required to identify all PII residing within their organization or under the control of their organization through a third party (e.g., a system being developed and tested by a contractor). Organizations should use a variety of methods to identify PII. Privacy threshold analyses (PTAs), also referred to as initial privacy assessments (IPAs), are often used to identify PII.[19] Some organizations require a PTA to be completed before the development or acquisition of a new information system and when a substantial change is made to an existing system. PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment (PIA) is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs are usually submitted to an organization's privacy office for review and approval. PTAs are comprised of simple questionnaires that are completed by the system owner in collaboration with the data owner. PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer. Other examples of methods to identify PII include reviewing system documentation, conducting interviews, conducting data calls, using data loss prevention technologies (e.g., automated PII network monitoring tools), or checking with system and data owners. Organizations should also ensure that retired hardware no longer contains PII and that proper sanitization techniques are applied.[20]

2.2 Examples of PII Data

The following list contains examples of information that may be considered PII.

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number[21]
- Address information, such as street address or email address
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
- Telephone numbers, including mobile, business, and personal numbers
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
- Information identifying personally owned property, such as vehicle registration number or title number and related information
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

[19] Some organizations have similar processes in place and do not call them PTA or IPA. For example PTA/IPA templates, see http://www.usdoj.gov/opcl/initial-privacy-assessment.pdf or http://www.dhs.gov/xlibrary/assets/privacy/privacy_pta_template.pdf.

[20] For more information on media sanitization, see NIST SP 800-88, *Guidelines for Media Sanitization*, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[21] Partial identifiers, such as the first few digits or the last few digits of SSNs, are also often considered PII because they are still nearly unique identifiers and are linked or linkable to a specific individual.

2.3 PII and Fair Information Practices

The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed. Treatment of PII is distinct from other types of data because it needs to be not only protected, but also collected, maintained, and disseminated in accordance with Federal law.[22] The Privacy Act, as well as other U.S. privacy laws, is based on the widely-recognized Fair Information Practices, also called Privacy Principles. The Organisation for Economic Co-operation and Development (OECD)[23] Privacy Guidelines are the most widely-accepted privacy principles, and they were endorsed by the Department of Commerce in 1981.[24] The OECD Fair Information Practices are also the foundation of privacy laws and related policies in many other countries, (e.g., Sweden, Australia, Belgium).[25] In 2004, the Chief Information Officers (CIO) Council issued the Security and Privacy Profile for the Federal Enterprise Architecture[26] that links privacy protection with a set of acceptable privacy principles corresponding to the OECD's Fair Information Practices.

The OECD identified the following Fair Information Practices.

- **Collection Limitation—**There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality—**Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
- **Purpose Specification—**The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation—**Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.
- **Security Safeguards—**Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Openness—**There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation—**An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given

[22] This document focuses on protecting the confidentiality of PII. Protecting the privacy of PII is a broader subject, and information about the Fair Information Practices is provided to increase reader awareness and to improve reader understanding of the relationship between privacy and security.

[23] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980.

[24] Report on OECD Guidelines Program, Memorandum from Bernard Wunder, Jr., Assistant Secretary for Communications and Information, Department of Commerce (Oct. 30, 1981), as cited in GAO Report 08-536.

[25] GAO Report 08-536.

[26] The Security and Privacy Profile was updated in 2009. For additional information, see Appendix D.

reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

- **Accountability—**A data controller should be accountable for complying with measures which give effect to the principles stated above.

Privacy is much broader than just protecting the confidentiality of PII. To establish a comprehensive privacy program that addresses the range of privacy issues that organizations may face, organizations should take steps to establish policies and procedures that address all of the Fair Information Practices. For example, while providing individuals with notice of new information collections and how their personal information will be used and protected is central to providing individuals with privacy protections and transparency, it may not have a significant impact on protecting the confidentiality of their personal information. On the other hand, the Fair Information Practices related to establishing security safeguards, purpose specification, use limitation, collection limitation, and accountability are directly relevant to the protection of the confidentiality of PII. As a result, these principles are highlighted throughout this document as appropriate.

For more information on the Fair Information Practices, see Appendix D.

3. PII Confidentiality Impact Levels

This publication focuses on protecting PII from losses of confidentiality. The security objective of confidentiality is defined by law as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[27]

The security objectives of integrity and availability are equally important for PII, and organizations should use the NIST Risk Management Framework[28] to determine the appropriate integrity and availability impact levels. Organizations may also need to consider PII-specific enhancements to the integrity or availability impact levels. Accuracy is a required Fair Information Practice for most PII, and the security objective of integrity helps to ensure accuracy. Integrity is also important for preventing harm to the individual and the organization. For example, unauthorized alterations of medical records could endanger individuals' lives, and medical mistakes based on inaccurate information can result in liability to the organization and harm to its reputation.

The confidentiality of PII should be protected based on its impact level. This section outlines factors for determining the PII confidentiality impact level for a particular instance of PII, which is distinct from the confidentiality impact level described in Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.[29] The PII confidentiality impact level takes into account additional PII considerations and should be used to determine if additional protections should be implemented. The PII confidentiality impact level—*low, moderate, or high*—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. Once the PII confidentiality impact level is selected, it should be used to supplement the provisional confidentiality impact level, which is determined from information and system categorization processes outlined in FIPS 199 and NIST Special Publication (SP) 800-60, *Volumes 1 and 2: Guide for Mapping Types of Information and Information Systems to Security Categories*.[30] Supplementation of the provisional confidentiality impact level should be included in the documentation of the security categorization process.

Some PII does not need to have its confidentiality protected, such as information that the organization has permission or authority to release publicly (e.g., an organization publishing a phone directory of employees' names and work phone numbers so that members of the public can contact them directly). In this case, the PII confidentiality impact level would be *not applicable* and would not be used to supplement a system's provisional confidentiality impact level. PII that does not require confidentiality protection may still require other security controls to protect the integrity and the availability of the information, and the organization should provide appropriate security controls based on the assigned FIPS 199 impact levels.

3.1 Impact Level Definitions

The harm caused from a breach of confidentiality should be considered when attempting to determine which PII confidentiality impact level corresponds to a specific set of PII. For the purposes of this document, *harm* means any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects (i.e., that may be socially, physically, or financially damaging). Examples of types of harm to individuals include, but are

[27] 44 U.S.C. § 3542, http://uscode.house.gov/download/pls/44C35.txt
[28] For additional information about the NIST Risk Management Framework, see: http://csrc.nist.gov/groups/SMA/fisma/framework.html.
[29] http://csrc.nist.gov/publications/PubsFIPS.html.
[30] http://csrc.nist.gov/publications/PubsSPs.html.

not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress. Organizations may also experience harm as a result of a loss of confidentiality of PII maintained by the organization, including but not limited to administrative burden, financial losses, loss of public reputation and public confidence, and legal liability.

The following describe the three impact levels—low, moderate, and high—defined in FIPS 199, which are based on the potential impact of a security breach involving a particular system:[31]

> "The potential impact is **LOW** if the loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
>
> The potential impact is **MODERATE** if the loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
>
> The potential impact is **HIGH** if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."

Harm to individuals as described in these impact levels is easier to understand with examples. A breach of the confidentiality of PII at the low impact level would not cause harm greater than inconvenience, such as changing a telephone number. The types of harm that could be caused by a breach involving PII at the moderate impact level include financial loss due to identity theft or denial of benefits, public humiliation, discrimination, and the potential for blackmail. Harm at the high impact level involves serious physical, social, or financial harm, resulting in potential loss of life, loss of livelihood, or inappropriate physical detention.

3.2 Factors for Determining PII Confidentiality Impact Levels[32]

Determining the impact from a loss of confidentiality of PII should take into account relevant factors. Several important factors that organizations should consider are described below. It is important to note that relevant factors should be considered together; one factor by itself might indicate a low impact level, but another factor might indicate a high impact level, and thus override the first factor. Also, the impact

[31] This document pertains only to the confidentiality impact and does not address integrity or availability.

[32] Portions of this section were submitted as contributions to the ISO/IEC 29101 *Privacy Reference Architecture* and the ISO/IEC 29100 *Privacy Framework* draft standards.

levels suggested for these factors are for illustrative purposes; each instance of PII is different, and each organization has a unique set of requirements and a different mission. Therefore, organizations should determine which factors, including organization-specific factors, they should use for determining PII confidentiality impact levels and should create and implement policy and procedures that support these determinations.

3.2.1 Identifiability

Organizations should evaluate how easily PII can be used to identify specific individuals. For example, PII data composed of individuals' names, fingerprints, or SSNs uniquely and directly identify individuals, whereas PII data composed of individuals' ZIP codes and dates of birth can indirectly identify individuals or can significantly narrow large datasets.[33] However, data composed of only individuals' area codes and gender usually would not provide for direct or indirect identification of an individual depending upon the context and sample size.[34] Thus, PII that is uniquely and directly identifiable may warrant a higher impact level than PII that is not directly identifiable by itself.

3.2.2 Quantity of PII

Organizations may also choose to consider how many individuals are identified in the information (e.g., number of records). Breaches of 25 records and 25 million records may have different impacts, not only in terms of the collective harm to individuals, but also in terms of harm to the organization's reputation and the cost to the organization in addressing the breach. For this reason, organizations may choose to set a higher impact level for particularly large PII datasets than would otherwise be set. However, organizations should not set a lower impact level for a PII dataset simply because it contains a small number of records.

3.2.3 Data Field Sensitivity

Organizations should evaluate the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together.[35] For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code. Organizations often require the PII confidentiality impact level to be set at least to moderate if a certain data field, such as SSN, is present. Organizations may also consider certain combinations of PII data fields to be more sensitive, such as name and credit card number, than each data field would be considered without the existence of the others. Data fields may also be considered more sensitive based on potential harm when used in contexts other than their intended use. For example, basic background information, such as place of birth or parent's middle name, is often used as an authentication factor for password recovery at many web sites.

[33] A Massachusetts Institute of Technology study showed that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth. L. Sweeney, *Computational Disclosure Control: A Primer on Data Privacy Protection*, Doctoral Dissertation, 2001, as cited in American Statistical Association, *Data Access and Personal Privacy: Appropriate Methods of Disclosure Control*, December 6, 2008, http://www.amstat.org/news/statementondataaccess.cfm.

[34] Section 4.2 discusses how organizations can reduce the need to protect PII by removing PII from records.

[35] Some organizations have defined certain types or categories of PII as sensitive and assign higher impact levels to those types of PII. For example, in its PIA policy, the Census Bureau has defined the following topics as sensitive: abortion; alcohol, drug, or other addictive products; illegal conduct; illegal immigration status; information damaging to financial standing, employability, or reputation; information leading to social stigmatization or discrimination; politics; psychological well-being or mental health; religion; same-sex partners; sexual behavior; sexual orientation; taxes; and other information due to specific cultural or other factors. http://www.census.gov/po/pia/pia_guide.html.

3.2.4 Context of Use

The context of use factor is related to the Fair Information Practices of Purpose Specification and Use Limitation. *Context of use* is defined as the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated. Examples of context include, but are not limited to, statistical analysis, eligibility for benefits, administration of benefits, research, tax administration, or law enforcement. Organizations should assess the context of use because it is important in understanding how the disclosure of data elements can potentially harm individuals and the organization. Organizations should also consider whether disclosure of the mere fact that PII is being collected or used could cause harm to the organization or individual. For example, law enforcement investigations could be compromised if the mere fact that information is being collected about a particular individual is disclosed.

The context of use factor may cause the same types of PII to be assigned different PII confidentiality impact levels in different instances. For example, suppose that an organization has three lists that contain the same PII data fields (e.g., name, address, phone number). The first list is people who subscribe to a general-interest newsletter produced by the organization. The second list is people who have filed for retirement benefits, and the third list is individuals who work undercover in law enforcement. The potential impacts to the affected individuals and to the organization are significantly different for each of the three lists. Based on context of use only, the three lists are likely to merit impact levels of low, moderate, and high, respectively.

3.2.5 Obligation to Protect Confidentiality

An organization that is subject to any obligations to protect PII should consider such obligations when determining the PII confidentiality impact level. Many organizations are subject to laws, regulations, or other mandates[36] governing the obligation to protect personal information,[37] such as the Privacy Act of 1974, OMB memoranda, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Additionally, some Federal agencies, such as the Census Bureau and the Internal Revenue Service (IRS), are subject to additional specific legal obligations to protect certain types of PII.[38] Some organizations are also subject to specific legal requirements based on their role. For example, organizations acting as financial institutions by engaging in financial activities are subject to the Gramm-Leach-Bliley Act (GLBA).[39] Also, some agencies that collect PII for statistical purposes are subject to the strict confidentiality requirements of the Confidential Information Protection and Statistical Efficiency Act (CIPSEA).[40] Violations of these laws can result in civil or criminal penalties. Organizations may also be obliged to protect PII by their own policies, standards, or management directives.

Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with an organization's legal counsel and privacy officer because relevant laws, regulations, and other mandates are often complex and change over time.

[36] See Appendix G for additional resources.

[37] Personal information is defined in different ways by different laws, regulations, and other mandates. Many of these definitions are not interchangeable. Therefore, it is important to use each specific definition to determine if an obligation to protect exists for each type of personal information. See Appendix C for a listing of common definitions of personal information.

[38] The Census Bureau has a special obligation to protect based on provisions of Title 13 of the U.S. Code, and the IRS has a special obligation to protect based on Title 26 of the U.S. Code. There are more agency-specific obligations to protect PII, and an organization's legal counsel and privacy officer should be consulted.

[39] For additional information, see GLBA, 15 U.S.C. § 6801 et seq.

[40] CIPSEA is Title 5 of the E-Government Act of 2002, Pub.L. 107-347, 116 Stat. 2899, 44 U.S.C. § 101 et seq. CIPSEA covers all types of data collected for statistical purposes, not just PII. For additional information, see the OMB Implementation Guidance for CIPSEA, http://www.whitehouse.gov/omb/fedreg/2007/061507_cipsea_guidance.pdf.

3.2.6 Access to and Location of PII

Organizations may choose to take into consideration the nature of authorized access to PII. When PII is accessed more often or by more people and systems, there are more opportunities for the confidentiality of the PII to be compromised. Another aspect of the nature of access to PII is whether PII is being stored on or accessed from teleworkers' devices or other systems and other systems, such as web applications, outside the direct control of the organization.[41] These considerations could cause an organization to assign a higher impact level to widely-accessed PII than would otherwise be assigned to help mitigate the increased risk caused by the nature of the access.

Additionally, organizations may choose to consider whether PII that is stored or regularly transported off-site by employees should be assigned a higher PII confidentiality impact level. For example, surveyors, researchers, and other field employees often need to store PII on laptops or removable media as part of their jobs. Another example is the offsite storage of backup and archive data. PII located offsite could be more vulnerable to unauthorized access or disclosure because it is more likely to be lost or stolen than PII stored within the physical boundaries of the organization.

3.3 PII Confidentiality Impact Level Examples

The following examples illustrate how an organization might assign PII confidentiality impact levels to specific instances of PII. The examples are intended to help organizations better understand the process of considering the various impact level factors, and they are not a substitute for organizations analyzing their own situations. Certain circumstances within any organization or specific system, such as the context of use or obligation to protect, may cause different outcomes.

Obligation to protect is a particularly important factor that should be determined early in the categorization process. Since obligation to protect confidentiality should always be made in consultation with an organization's legal counsel and privacy officer, it is not addressed in the following examples.

3.3.1 Example 1: Incident Response Roster

A Federal government agency maintains an electronic roster of its computer incident response team members. In the event that an IT staff member detects any kind of security breach, standard practice requires that the staff member contact the appropriate people listed on the roster. Because this team may need to coordinate closely in the event of an incident, the contact information includes names, professional titles, office and work cell phone numbers, and work email addresses. The agency makes the same types of contact information available to the public for all of its employees on its main web site.

Identifiability: The information directly identifies a small number of individuals using names, phone numbers, and email addresses.

Quantity of PII: The information directly identifies fewer than twenty individuals.

Data field sensitivity: Although the roster is intended to be made available only to the team members, the individuals' information included in the roster is already available to the public on the agency's web site.

[41] Systems containing PII that are owned and/or maintained at contractor site for a Federal agency are subject to same controls and authorization requirements as if the systems were located at a Federal agency site. See NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach,* http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

Context of use: The release of the individuals' names and contact information would not likely cause harm to the individuals, and disclosure of the fact that the agency has collected or used this information is also unlikely to cause harm.

Access to and location of PII: The information is accessed by IT staff members who detect security breaches, as well as the team members themselves. The PII needs to be readily available to teleworkers and to on-call IT staff members so that incident responses can be initiated quickly.

Taking into account these factors, the agency determines that unauthorized access to the roster would likely cause little or no harm, and it chooses to assign the PII confidentiality impact level of *low*.[42]

3.3.2 Example 2: Intranet Activity Tracking

An organization maintains a web use audit log for an intranet web site accessed by employees. The web use audit log contains the following:

- The user's IP address
- The Uniform Resource Locator (URL) of the web site the user was viewing immediately before coming to this web site (i.e., referring URL)
- The date and time the user accessed the web site
- The web pages or topics accessed within the organization's web site (e.g., organization security policy).

Identifiability: By itself, the log does not contain any directly identifiable data. However, the organization has a closely-related system with a log that contains domain login information records, which include user IDs and corresponding IP addresses. Administrators who have access to both systems and their logs could correlate information between the logs and identify individuals. Potentially, information could be stored about the actions of most of the organization's users involving web access to intranet resources. The organization has a small number of administrators who have access to both systems and both logs.

Quantity of PII: The log contains a large number of records containing linked PII.

Data field sensitivity: The information on which internal web pages and topics were accessed could potentially cause some embarrassment if the pages involved certain human resources-related subjects, such as a user searching for information on substance abuse programs. However, since the logging is limited to use of intranet-housed information, the amount of potentially embarrassing information is minimal.

Context of use: Creation of the logs is known to all staff members through the organization's acceptable use policies. The release of the information would be unlikely to cause harm, other than potential embarrassment for a small number of users.

Access to and location of PII: The log is accessed by a small number of system administrators when troubleshooting operational problems and also occasionally by a small number of incident response

[42] This scenario is presented for illustrative purposes only. It is possible that this type of information could be used for a social engineering attack. Organizations may consider their particular circumstances and assign a higher impact level for this scenario.

personnel when investigating incidents. All access to the log occurs only from the organization's own systems.

Taking into account these factors, the organization determines that a breach of the log's confidentiality would likely cause little or no harm, and it chooses to assign the PII confidentiality impact level of *low*.

3.3.3 Example 3: Fraud, Waste, and Abuse Reporting Application

A database contains web form submissions by individuals claiming possible fraud, waste, or abuse of organizational resources and authority. Some of the submissions include serious allegations, such as accusing individuals of accepting bribes or not enforcing safety regulations. The submission of contact information is not prohibited, and individuals often enter their personal information in the form's narrative text field. The web site is hosted by a server that logs IP address and referring web site information.

Identifiability: By default, the database does not request PII, but a significant percentage of users choose to provide PII. The web log contains IP addresses, which could be identifiable. However, the log information is not linked or readily linkable with the database or other sources to identify specific individuals.

Quantity of PII: A recent estimate indicated that the database has approximately 50 records with PII out of nearly 1000 total records.

Data field sensitivity: The database's narrative text field contains user-supplied text and frequently includes information such as name, mailing address, email address, and phone numbers.

Context of use: Because of the nature of the submissions (i.e., reporting claims of fraud, waste, or abuse), the disclosure of individuals' identities would likely cause some of the individuals making the claims to fear retribution by management and peers. Additionally, it could negatively impact individuals about whom accusations are made. The ensuing harm could include blackmail, severe emotional distress, loss of employment, and physical harm. A breach would also undermine employee and public trust in the organization.

Access to and location of PII: The database is only accessed by a few people who investigate fraud, waste, and abuse claims. All access to the database occurs only from the organization's internal systems.

Taking into account these factors, the organization determines that a breach of the database's confidentiality would likely cause catastrophic harm to some of the individuals and chooses to assign the PII confidentiality impact level of *high*.

4. PII Confidentiality Safeguards

PII should be protected through a combination of measures, including operational safeguards, privacy-specific safeguards, and security controls. Many of these measures also correspond to several of the Fair Information Practices. Organizations should use a risk-based approach for protecting the confidentiality of PII. The PII safeguards provided in this section are complementary to other safeguards for data and may be used as one part of an organization's comprehensive approach to protecting the confidentiality of PII and implementing the Fair Information Practices.

4.1 Operational Safeguards

This section describes two types of operational safeguards for PII protection: policy and procedure creation; and education, training, and awareness. Organizations can choose whether these policy, education, and awareness activities are combined with related security controls (e.g., AT-1, AT-2) or are separated as part of a privacy program.

As agencies work to establish a variety of safeguards to protect the confidentiality of PII, they must also ensure that mechanisms are in place to make certain that individuals are held accountable for implementing these controls adequately and that the controls are functioning as intended. Accountability is also an important Fair Information Practice. In this context, agencies may already have some pre-established processes for providing oversight and accountability for the implementation of key controls, such as those related to information system assessment and authorization, Privacy Impact Assessments, and Privacy Act compliance. However, some additional oversight mechanisms or amendments to pre-existing procedures could be necessary to ensure that all measures for protecting PII are being considered and properly implemented.

4.1.1 Policy and Procedure Creation

Organizations should develop comprehensive policies and procedures for handling PII at the organization level, the program or component level, and where appropriate, at the system level.[43] Some types of policies include foundational privacy principles, privacy rules of behavior, policies that implement laws and other mandates, and system-level policies. The foundational privacy principles reflect the organization's privacy objectives. Foundational privacy principles may also be used as a guide against which to develop additional policies and procedures. Privacy rules of behavior policies provide guidance on the proper handling of PII, as well as the consequences for failure to comply with the policy. Some policies provide guidance on implementing laws and OMB guidance in an organization's environment based upon the organization's authorized business purposes and mission. Organizations should consider developing privacy policies and associated procedures for the following topics:

- Access rules for PII within a system
- PII retention schedules and procedures
- PII incident response and data breach notification

[43] There are laws and OMB guidance that provide agency requirements for policy development. For example, OMB Memorandum 05-08 requires that a "senior agency official must…have a central policy-making role in the agency's development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues…." Additionally, the Privacy Act requires agencies to "establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of…" the Privacy Act "including any other rules and procedures adopted…and the penalties for noncompliance." 5 U.S.C. § 552a(e)(9).

- Privacy in the system development life cycle process
- Limitation of collection, disclosure, sharing, and use of PII
- Consequences for failure to follow privacy rules of behavior.

If the organization permits access to or transfer of PII through interconnected systems external to the organization or shares PII through other means, the organization should implement the appropriate documented agreements for roles and responsibilities, restrictions on further sharing of the information, requirements for notification to each party in the case of a breach, minimum security controls, and other relevant factors. Also, Interconnection Security Agreements (ISA) should be used for technical requirements as necessary.[44] These agreements ensure that the partner organizations abide by rules for handling, disclosing, sharing, transmitting, retaining, and using the organization's PII.

PII maintained by the organization should also be reflected in the organization's incident response policies and procedures. A well-defined incident response capability helps the organization detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly. OMB M-07-16 sets out specific requirements for reporting incidents involving the loss or inappropriate disclosure of PII. For additional information, see Section 5.

4.1.2 Awareness, Training, and Education

Awareness, training, and education are distinct activities, each critical to the success of privacy and security programs.[45] Their roles related to protecting PII are briefly described below. Additional information on privacy education, training, and awareness is available in NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*.

Awareness efforts are designed to change behavior or reinforce desired PII practices. The purpose of awareness is to focus attention on the protection of PII. Awareness relies on using attention-grabbing techniques to reach all different types of staff across an organization. For PII protection, awareness methods include informing staff of new scams that are being used to steal identities, providing updates on privacy items in the news such as government data breaches and their effect on individuals and the organization, providing examples of how staff members have been held accountable for inappropriate actions, and providing examples of recommended privacy practices.

The goal of training is to build knowledge and skills that will enable staff to protect PII. Laws and regulations may specifically require training for staff, managers, and contractors. An organization should have a training plan and implementation approach, and an organization's leadership should communicate the seriousness of protecting PII to its staff. Organizational policy should define roles and responsibilities for training; training prerequisites for receiving access to PII; and training periodicity and refresher training requirements. To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that have been granted access to PII should receive appropriate training and, where applicable, specific role-based training. Depending on the roles and functions involving PII, important topics to address may include:

- The definition of PII

[44] See NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, http://csrc.nist.gov/publications/PubsSPs.html.

[45] Some organizations have chosen to combine their security and privacy awareness, education, and training, whereas other organizations have chosen to keep them separate. Additionally, the Privacy Act and OMB guidance specifically require privacy training.

- Applicable privacy laws, regulations, and policies
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Appropriate disposal of PII
- Sanctions for misuse of PII
- Recognition of a security or privacy incident involving PII
- Retention schedules for PII
- Roles and responsibilities in responding to PII-related incidents and reporting.

Education develops a common body of knowledge that reflects all of the various specialties and aspects of PII protection. It is used to develop privacy professionals who are able to implement privacy programs that enable their organizations to proactively respond to privacy challenges.

4.2 Privacy-Specific Safeguards[46]

Privacy-specific safeguards are controls for protecting the confidentiality of PII. These controls provide types of protections not usually needed for other types of data. Privacy-specific safeguards help organizations collect, maintain, use, and disseminate data in ways that protect the confidentiality of the data.

4.2.1 Minimizing the Use, Collection, and Retention of PII

The practice of minimizing the use, collection, and retention of PII is a basic privacy principle.[47] By limiting PII collections to the least amount necessary to conduct its mission, the organization may limit potential negative consequences in the event of a data breach involving PII. Organizations should consider the total amount of PII used, collected, and maintained, as well as the types and categories of PII used, collected, and maintained. This general concept is often abbreviated as the "minimum necessary" principle. PII collections should only be made where such collections are essential to meet the authorized business purpose and mission of the organization. If the PII serves no current business purpose, then the PII should no longer be used or collected.

Also, an organization should regularly review[48] its holdings of previously collected PII to determine whether the PII is still relevant and necessary for meeting the organization's business purpose and mission.[49] If PII is no longer relevant and necessary, then PII should be properly destroyed. The destruction or disposal of PII must be conducted in accordance with any litigation holds and the Federal Records Act and records control schedules approved by the National Archives and Records Administration (NARA).[50] Organizations should also ensure that retired hardware has been properly

[46] Portions of this section were submitted as contributions to the ISO/IEC 29100 *Privacy Framework* draft standard.

[47] Fair Information Practices are also referred to as privacy principles. See Appendix D for additional information.

[48] The frequency of reviews should be done in accordance with laws, regulations, mandates, and organizational policies that apply to the collection of PII.

[49] The Privacy Act requires that Federal agencies only maintain records relevant and necessary to their mission. 5 U.S.C. § 552a(e)(1). Also, OMB directed Federal agencies to review their PII holdings annually and to reduce their holdings to the minimum necessary for proper performance of their missions. OMB M-07-16.

[50] The Federal Records Act, 44 U.S.C. § 3301, defines records as "[a]ll books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or

sanitized before disposal (e.g., no disk images contain PII, the hard drive has been properly sanitized).[51] The effective management and prompt disposal of PII, in accordance with NARA-approved disposition schedules, will minimize the risk of unauthorized disclosure.

4.2.2 Conducting Privacy Impact Assessments

PIAs are structured processes for identifying and mitigating privacy risks, including risks to confidentiality, within an information system. According to OMB, PIAs are "structured reviews of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form[52] in an electronic information system, and (iii) to identify and evaluate protections and alternative processes for handling information to mitigate potential privacy risks."[53] If used effectively, a PIA should address confidentiality risks at every stage of the system development life cycle (SDLC). Many organizations have established their own templates that provide the basis for conducting a PIA. The following are some topics that are commonly addressed through the use of a PIA:

- What information is to be collected
- Why the information is being collected
- The intended use of the information
- With whom the information will be shared
- How the information will be secured
- What choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

4.2.3 De-Identifying Information

Full data records are not always necessary, such as for some forms of research, resource planning, and examinations of correlations and trends. The term *de-identified information* is used to describe records that have had enough PII removed or *obscured*, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.[54] De-identified information can be re-identified

appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them." Agencies are required to create and maintain "adequate and proper documentation" of their organization, mission, functions, etc., and may not dispose of records without the approval of the Archivist of the United States. This approval is granted through the General Records Schedules (GRS) and agency specific records schedules.

[51] For more information on media sanitization, see NIST SP 800-88, *Guidelines for Media Sanitization*, http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

[52] See Appendix C for additional information about information in identifiable form (IIF).

[53] OMB M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, http://www.whitehouse.gov/omb/memoranda/m03-22.html. For additional PIA information specific to Federal agencies, see Appendix B.

[54] For the purpose of analysis, the definition for de-identified information used in this document is loosely based on the requirements for de-identified data defined in the HIPAA Privacy Rule, and it is generalized to apply to all PII. This definition differs from the HIPAA definition in that it is applied to all PII and does not specifically require the removal of all 18 data elements described by the HIPAA Privacy Rule. The HIPAA Privacy Rule recognizes two ways to de-identify data such that it is no longer considered to be protected health information (PHI). First, 18 specific fields can be removed, such as name, SSN, and phone number. Second, a person with appropriate knowledge and experience in statistical methods

(rendered distinguishable) by using a code, algorithm, or pseudonym that is assigned to individual records. The code, algorithm, or pseudonym should not be derived from other related information[55] about the individual, and the means of re-identification should only be known by authorized parties and not disclosed to anyone without the authority to re-identify records. A common de-identification technique for obscuring PII is to use a one-way cryptographic function, also known as a hash function, on the PII.[56] De-identified information can be assigned a PII confidentiality impact level of *low*, as long as the following are both true:

- The re-identification algorithm, code, or pseudonym is maintained in a separate system, with appropriate controls in place to prevent unauthorized access to the re-identification information.
- The data elements are not linkable, via public records or other reasonably available external records, in order to re-identify the data.

For example, de-identification could be accomplished by removing account numbers, names, SSNs, and any other identifiable information from a set of financial records. By de-identifying the information, a trend analysis team could perform an unbiased review on those records in the system without compromising the PII or providing the team with the ability to identify any individual. Another example is using health care test results in research analysis. All of the identifying PII fields can be removed, and the patient ID numbers can be obscured using pseudo-random data that is associated with a cross-reference table located in a separate system. The only means to reconstruct the original (complete) PII records is through authorized access to the cross-reference table.

Additionally, de-identified information can be aggregated for the purposes of statistical analysis, such as making comparisons, analyzing trends, or identifying patterns. An example is the aggregation and use of multiple sets of de-identified data for evaluating several types of education loan programs. The data describes characteristics of loan holders, such as age, gender, region, and outstanding loan balances. With this dataset, an analyst could draw statistics showing that 18,000 women in the 30-35 age group have outstanding loan balances greater than $10,000. Although the original dataset contained distinguishable identities for each person, the de-identified and aggregated dataset would not contain linked or readily identifiable data for any individual.

4.2.4 Anonymizing Information

Anonymized information[57] is defined as previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists.[58] Anonymizing information

applies de-identification methods, determines the risk is very small, and documents the justification. 45 C.F.R. § 164.514, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

[55] This is not intended to exclude the application of cryptographic hash functions to the information.

[56] Hashing may not be appropriate for de-identifying information covered by HIPAA. 45 C.F.R. § 164.514 (c)(1) specifically excludes de-identification techniques where the code is derived from the PII itself. Organizations should consult their legal counsel for legal requirements related to de-identification and anonymization.

[57] For additional information about anonymity, see: A. Pfitzmann and M. Hansen, *A Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management*, updated 2009, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.32.pdf.

[58] Based on the Common Rule, which governs confidentiality requirements for research, 15 C.F.R. Part 27. Some organizations do not distinguish between the terms de-identified and anonymized information and use them interchangeably. Additionally, the amount of information available publicly and advances in computational technology make full anonymity of released datasets (e.g., census data and public health data) difficult to accomplish. For additional information, see: American Statistical Association, *Data Access and Personal Privacy: Appropriate Methods of Disclosure Control*, December 6, 2008, http://www.amstat.org/news/statementondataaccess.cfm.

usually involves the application of statistical disclosure limitation techniques[59] to ensure the data cannot be re-identified, such as:[60]

- **Generalizing the Data—**Making information less precise, such as grouping continuous values
- **Suppressing the Data—**Deleting an entire record or certain parts of records
- **Introducing Noise into the Data—**Adding small amounts of variation into selected data
- **Swapping the Data—**Exchanging certain data fields of one record with the same data fields of another similar record (e.g., swapping the ZIP codes of two records)
- **Replacing Data with the Average Value—**Replacing a selected value of data with the average value for the entire group of data.

Using these techniques, the information is no longer PII, but it can retain its useful and realistic properties.[61]

Anonymized information is useful for system testing.[62] Systems that are newly developed, newly purchased, or upgraded require testing before being introduced to their intended production (or live) environment. Testing generally should simulate real conditions as closely as possible to ensure the new or upgraded system runs correctly and handles the projected system capacity effectively. If PII is used in the test environment, it is required to be protected at the same level that it is protected in the production environment, which can add significantly to the time and expense of testing the system.

Randomly generating fake data in place of PII to test systems is often ineffective because certain properties and statistical distributions of PII may need to be retained to effectively test the system. There are tools available that substitute PII with synthetic data generated by anonymizing PII. The anonymized information retains the useful properties of the original PII, but the anonymized information is not considered to be PII. Anonymized data substitution is a privacy-specific protection measure that enables system testing while reducing the expense and added time of protecting PII. However, not all data can be readily anonymized (e.g., biometric data).

4.3 Security Controls

In addition to the PII-specific safeguards described earlier in this section, many types of security controls are available to safeguard the confidentiality of PII. Providing reasonable security safeguards is also a Fair Information Practice. Security controls are often already implemented on a system to protect other types of data processed, stored, or transmitted by the system. The security controls listed in NIST SP 800-53 address general protections of data and systems. The items listed below are some of the NIST SP 800-53 controls that can be used to help safeguard the confidentiality of PII. Note that some of these

[59] Both anonymizing and de-identifying should be conducted by someone with appropriate training. It may be helpful, as appropriate, to consult with a statistician to assess the level of risk with respect to possible unintended re-identification and improper disclosure. For additional information on statistical disclosure limitation techniques, see OMB's Statistical Policy Working Paper #22, http://www.fcsm.gov/working-papers/spwp22.html. See also Census Bureau, *Report on Confidentiality* and Privacy 1790-2002, http://www.census.gov/prod/2003pubs/conmono2.pdf.

[60] The Federal Committee on Statistical Methodology provides a checklist to assist in the assessment of risk for re-identification and improper disclosure. For additional information, see the Federal Committee on Statistical Methodology: Confidentiality and Data Access Committee, *Checklist on Disclosure Potential of Data Releases*, http://www.fcsm.gov/committees/cdac/.

[61] The retention of useful properties in anonymized data is dependent upon the statistical disclosure limitation technique applied.

[62] Anonymization is also commonly used by agencies to release datasets to the public for research purposes.

controls may not be in the recommended set of security controls for the baselines identified in NIST SP 800-53 (e.g., a control might only be recommended for high-impact systems). However, organizations may choose to provide greater protections than what is recommended; see Section 3.2 for a discussion of factors to consider when choosing the appropriate controls. In addition to the controls listed below, NIST SP 800-53 contains many other controls that can be used to help protect PII, such as incident response controls.

- **Access Enforcement (AC-3).** Organizations can control access to PII through access control policies and access enforcement mechanisms (e.g., access control lists). This can be done in many ways. One example is implementing role-based access control and configuring it so that each user can access only the pieces of data necessary for the user's role. Another example is only permitting users to access PII through an application that tightly restricts their access to the PII, instead of permitting users to directly access the databases or files containing PII.[63] Encrypting stored information is also an option for implementing access enforcement.[64] OMB M-07-16 specifies that Federal agencies must "encrypt, using only NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary or a senior-level individual he/she may designate in writing".

- **Separation of Duties (AC-5).** Organizations can enforce separation of duties for duties involving access to PII. For example, the users of de-identified PII data would not also be in roles that permit them to access the information needed to re-identify the records.

- **Least Privilege (AC-6).** Organizations can enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. Concerning PII, the organization can ensure that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- **Remote Access (AC-17).** Organizations can choose to prohibit or strictly limit remote access to PII. If remote access is permitted, the organization should ensure that the communications are encrypted.

- **User-Based Collaboration and Information Sharing (AC-21).** Organizations can provide automated mechanisms to assist users in determining whether access authorizations match access restrictions, such as contractually-based restrictions, for PII.

- **Access Control for Mobile Devices (AC-19).** Organizations can choose to prohibit or strictly limit access to PII from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDA), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities). Some organizations may choose to restrict remote access involving higher-impact instances of PII so that the information will not leave the organization's physical boundaries. If access is permitted, the organization can ensure that the devices are properly secured and regularly scan the devices to verify their security status (e.g., anti-malware software enabled and up-to-date, operating system fully patched).

- **Auditable Events (AU-2).** Organizations can monitor events that affect the confidentiality of PII, such as unauthorized access to PII.

[63] For example, suppose that an organization has a database containing thousands of records on employees' benefits. Instead of allowing a user to have full and direct access to the database, which could allow the user to save extracts of the database records to the user's computer, removable media, or other locations, the organization could permit the user to access only the necessary records and record fields. A user could be restricted to accessing only general demographic information and not any information related to the employees' identities.

[64] Additional encryption guidelines and references can be found in FIPS 140-2: *Security Requirements for Cryptographic Modules*, http://csrc.nist.gov/publications/PubsFIPS.html.

- **Audit Review, Analysis, and Reporting (AU-6)**. Organizations can regularly review and analyze information system audit records for indications of inappropriate or unusual activity affecting PII, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

- **Identification and Authentication (Organizational Users) (IA-2).** Users can be uniquely identified and authenticated before accessing PII.[65] The strength requirement for the authentication mechanism depends on the impact level of the PII and the system as a whole. OMB M-07-16 specifies that Federal agencies must “allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access,” and also must “use a ‘time-out’ function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity.”

- **Media Access (MP-2).** Organizations can restrict access to information system media containing PII, including digital media (e.g., CDs, USB flash drives, backup tapes) and non-digital media (e.g., paper, microfilm). This could also include portable and mobile devices with a storage capability.

- **Media Marking (MP-3).** Organizations can label information system media and output containing PII to indicate how it should be distributed and handled. The organization could exempt specific types of media or output from labeling so long as it remains within a secure environment. Examples of labeling are cover sheets on printouts and paper labels on digital media.

- **Media Storage (MP-4).** Organizations can securely store PII, both in paper and digital forms, until the media are destroyed or sanitized using approved equipment, techniques, and procedures. One example is the use of storage encryption technologies to protect PII stored on removable media.

- **Media Transport (MP-5).** Organizations can protect digital and non-digital media and mobile devices containing PII that is transported outside the organization’s controlled areas. Examples of protective safeguards are encrypting stored information and locking the media in a container.

- **Media Sanitization (MP-6).** Organizations can sanitize digital and non-digital media containing PII before it is disposed or released for reuse.[66] An example is degaussing a hard drive—applying a magnetic field to the drive to render it unusable.

- **Transmission Confidentiality (SC-9).** Organizations can protect the confidentiality of transmitted PII. This is most often accomplished by encrypting the communications or by encrypting the information before it is transmitted.[67]

- **Protection of Information at Rest (SC-28).** Organizations can protect the confidentiality of PII at rest, which refers to information stored on a secondary storage device, such as a hard drive or backup tape. This is usually accomplished by encrypting the stored information.

- **Information System Monitoring (SI-4).** Organizations can employ automated tools to monitor PII internally or at network boundaries for unusual or suspicious transfers or events. An example is the use of data loss prevention technologies.

[65] For additional information about authentication, see NIST SP 800-63, *Electronic Authentication Guideline*.

[66] For more information on media sanitization, see NIST SP 800-88, *Guidelines for Media Sanitization*.

[67] NIST has several publications on this topic that are available from http://csrc.nist.gov/publications/PubsSPs.html.

5. Incident Response for Breaches Involving PII

Handling incidents and breaches involving PII is different from regular incident handling and may require additional actions by an organization.[68] Breaches involving PII can receive considerable media attention, which can greatly harm an organization's reputation and reduce the public's trust[69] in the organization. Moreover, affected individuals can be subject to embarrassment, identity theft, or blackmail as the result of a breach involving PII. Due to these particular risks of harm, organizations should develop additional policies, such as determining when and how individuals should be notified, when and if a breach should be reported publicly, and whether to provide remedial services, such as credit monitoring, to affected individuals. Organizations should integrate these additional policies into their existing incident handling response policies.[70]

Management of incidents involving PII often requires close coordination among personnel from across the organization, such as the CIO, CPO, system owner, data owner, legal counsel, and public relations officer. Because of this need for close coordination, organizations should establish clear roles and responsibilities to ensure effective management when an incident occurs.

FISMA requires Federal agencies to have procedures for handling information security incidents, and it directed OMB to ensure the establishment of a central Federal information security incident center, which is the U.S. Computer Emergency Readiness Team (US-CERT). Additionally, NIST provided guidance on security incident handling in NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*. In 2007, OMB issued M-07-16, which provided specific guidance to Federal agencies for handling incidents involving PII.[71]

Incident response plans should be modified to handle breaches involving PII. Incident response plans should also address how to minimize the amount of PII necessary to adequately report and respond to a breach. NIST SP 800-61 Revision 1 describes four phases of handling security incidents. Specific policies and procedures for handling breaches involving PII can be added to each of the following phases identified in NIST SP 800-61: preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity. This section provides additional details on PII-specific considerations for each of these four phases.

5.1 Preparation

Preparation requires the most effort because it sets the stage to ensure the breach is handled appropriately. Organizations should build their response plans for breaches involving PII into their existing incident response plans. The development of response plans for breaches involving PII requires organizations to make many decisions about how to handle breaches involving PII, and the decisions should be used to develop policies and procedures. The policies and procedures should be communicated to the organization's entire staff through training and awareness programs. Training may include tabletop

[68] For the purposes of this document, incident and breach are used interchangeably to mean any violation or imminent threat of violation of privacy or computer security policies, acceptable use policies, privacy rules of behavior, or standard computer security practices. Modified from NIST SP 800-61 Revision 1.

[69] According to a 2007 Government Privacy Trust Survey conducted by the Ponemon Institute, a Federal department fell from being a top five most trusted agency in 2006 to just above the bottom five least trusted agencies after the highly publicized breach of millions of PII records in 2006. http://www.govexec.com/dailyfed/0207/022007tdpm1.htm.

[70] Some organizations choose to have separate policies and procedures for incidents and breaches of PII, which may involve the use of a separate privacy incident response team. If the policies and procedures are separate for incidents and breaches involving PII, then the security incident response plan should be amended so that staff members know when to follow the separate policies and procedures for incidents and breaches involving PII.

[71] Organizations may also want to review *Combating ID Theft: A Strategic Plan* from the President's Task Force on Identity Theft, April 2007, at: http://www.idtheft.gov/.

exercises to simulate an incident and test whether the response plan is effective and whether the staff members understand and are able to perform their roles effectively. Training programs should also inform employees of the consequences of their actions for inappropriate use and handling of PII.

The organization should determine if existing processes are adequate, and if not, establish a new incident reporting method for employees to report suspected or known incidents involving PII. The method could be a phone hotline, email, online form, or a management reporting structure in which employees know to contact a specific person within the management chain. Employees should be able to report any breach involving PII immediately on any day, at any time. Additionally, employees should be provided with a clear definition of what constitutes a breach involving PII and what information needs to be reported. The following information is helpful to obtain from employees who are reporting a known or suspected breach involving PII.[72]

- Person reporting the incident
- Person who discovered the incident
- Date and time the incident was discovered
- Nature of the incident
- Name of system and possible interconnectivity with other systems
- Description of the information lost or compromised
- Storage medium from which information was lost or compromised
- Controls in place to prevent unauthorized use of the lost or compromised information
- Number of individuals potentially affected
- Whether law enforcement was contacted.

Federal agencies are required to report all known or suspected breaches involving PII, in any format, to US-CERT within one hour.[73] To meet this obligation, organizations should proactively plan their breach notification response. A breach involving PII may require notification to persons external to the organization, such as law enforcement, financial institutions, affected individuals, the media, and the public.[74] Organizations should plan in advance how, when, and to whom notifications should be made. Organizations should conduct training sessions on interacting with the media regarding incidents. Additionally, OMB M-07-16 requires federal agencies to include the following elements in their plans for handling breach notification:

- Whether breach notification to affected individuals is required[75]
- Timeliness of the notification
- Source of the notification
- Contents of the notification

[72] U.S. Department of Commerce, *Breach Notification Response Plan*, September 28, 2007

[73] In M-07-16, OMB required Federal agencies to report all known or suspected PII breaches to US-CERT within one hour. This document does not change or affect any US-CERT reporting requirements as required by OMB, other NIST guidance, US-CERT, or statute.

[74] For additional information about communications with external parties, such as the media, see NIST SP 800-61 Revision 1.

[75] For Federal agencies, notification to US-CERT is always required.

- Means of providing the notification
- Who receives the notification; public outreach response
- What actions were taken and by whom

Additionally, organizations should establish a committee or person responsible for using the breach notification policy to coordinate the organization's response. Organizations also need to determine how incidents involving PII will be tracked within the organization.

The organization should also determine what circumstances require the organization to provide remedial assistance to affected individuals, such as credit monitoring services. The PII confidentiality impact level should be considered for this determination because it provides an analysis of the likelihood of harm for the loss of confidentiality for each instance of PII.

5.2 Detection and Analysis

Organizations may continue to use their current detection and analysis technologies and techniques for handling incidents involving PII. However, adjustments to incident handling processes may be necessary, such as ensuring that the analysis process includes an evaluation of whether an incident involves PII. Detection and analysis should focus on both known and suspected breaches involving PII. Detection of an incident involving PII also requires reporting internally, to US-CERT, and externally, as appropriate.

5.3 Containment, Eradication, and Recovery

Existing technologies and techniques for containment, eradication, and recovery may be used for breaches involving PII. However, changes to incident handling processes may be necessary, such as performing additional media sanitization steps when PII needs to be deleted from media during recovery. [76] PII should not be sanitized until a determination has been made about whether the PII must be preserved as evidence.[77] Particular attention should be paid to using proper forensics techniques[78] to ensure preservation of evidence. Additionally, it is important to determine whether PII was accessed and how many records or individuals were affected.

5.4 Post-Incident Activity

As with other security incidents, information learned through detection, analysis, containment, and recovery should be collected for sharing within the organization and with the US-CERT to help protect against future incidents. The incident response plan should be continually updated and improved based on the lessons learned during each incident. Lessons learned might also indicate the need for additional training, security controls, or procedures to protect against future incidents.

Additionally, the organization should use its response policy, developed during the planning phase, to determine whether the organization should provide affected individuals with remedial assistance. When providing notice to individuals, organizations should make affected individuals aware of their options,

[76] For additional information on media sanitization, see NIST SP 800-88.

[77] Often, information involved with an incident will need to be preserved in preparation for prosecution or litigation related to the incident. Legal counsel should be consulted before any PII is sanitized.

[78] For additional information, see NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf.

such as obtaining a free copy of their credit report, obtaining a freeze credit report, placing a fraud alert on their credit report, or contacting their financial institutions.[79]

[79] Organizations may need to provide other types of remedial assistance for breaches that would cause harm unrelated to identity theft and financial crimes, such as PII maintained for law enforcement, medical care, or homeland security.

Appendix A—Scenarios for PII Identification and Handling

Exercises involving PII scenarios within an organization provide an inexpensive and effective way to build skills necessary to identify potential issues with how the organization identifies and safeguards PII. Individuals who participate in these exercises are presented with a brief PII scenario and a list of general and specific questions related to the scenario. After reading the scenario, the group then discusses each question and determines the most appropriate response for their organization. The goal is to determine what the participants would really do and to compare that with policies, procedures, and generally recommended practices to identify any discrepancies or deficiencies and decide upon appropriate mitigation techniques.

The general questions listed below are applicable to almost any PII scenario. After the general questions are scenarios, each of which is followed by additional scenario-specific questions. Organizations are encouraged to adapt these questions and scenarios for use in their own PII exercises. Also, additional scenarios and questions specific to PII incident handling are available from NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*.[80]

A.1 General Questions

1. What procedures are in place to identify, assess, and protect the PII described in the scenario?

2. Which individuals have designated responsibilities within the organization to safeguard the PII described in the scenario?

3. To which people and groups within the organization should questions about PII or the possible misuse of PII be reported?

4. What could happen if the PII described in the scenario is not safeguarded properly?

A.2 Scenarios

Scenario 1: A System Upgrade

An organization is redesigning and upgrading its physical access control systems, which consist of entry-way consoles that recognize ID badges, along with identity management systems and other components. As part of the redesign, several individual physical access control systems are being consolidated into a single system that catalogues and recognizes biometric template data (a facial image and fingerprint), employee name, employee identification number (an internal identification number used by the organization) and employee SSN. The new system will also contain scanned copies of "identity" documentation, including birth certificates, driver's licenses, and/or passports. In addition, the system will maintain a log of all access (authorized or unauthorized) attempts by a badge. The log contains employee identification numbers and timestamps for each access attempt.

1. What information in the system is PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

[80] SP 800-61 Revision 1 is available at http://csrc.nist.gov/publications/PubsSPs.html.

3. By consolidating data into a single system, does it create additional vulnerabilities that could result in harm to the individual? What additional controls could be put in place to mitigate the risk?

4. Is all of the information necessary for the system to function? Is there a way to minimize the information in the system? Could PII on the system be replaced with anonymized data that is not PII?

5. Is the organization required to conduct a PIA for this system?

Scenario 2: Protecting Survey Data

Recently, an organization emailed to individuals a link to an online survey, which was designed to gather feedback about the organization's services. The organization identified each individual by name, email address, and an organization-assigned ID number. The majority of survey questions asked individuals to express their satisfaction or dissatisfaction with the organization, but there were also questions asking individuals to provide their ZIP code along with demographic details on their age, income level, educational background, and marital status.

The following are additional questions for this scenario:

1. Which data elements collected through this survey should be considered PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

3. How are determinations made as to which data from the survey is relevant to the organization's operations? Does the Paperwork Reduction Act apply? What happens to data that is deemed unnecessary?

4. What privacy-specific safeguards might help protect the PII collected and retained from this survey?

5. What other types of controls for safeguarding data (that are not necessarily specific to safeguarding PII) might be used to protect the data from the responses?

Scenario 3: Completing Work at Home

An organization's employee needed to leave early for a doctor's appointment, but the employee was not finished with her work for the day and had no leave time available. Since she had the same spreadsheet application at home, she decided to email a data extract as an attachment to her personal email address and finish her work at home that evening. The data extract was downloaded from an access-controlled human resources database located on a server within the organization's security perimeter. The extract contained employee names, identification numbers, dates of birth, salary information, manager names, addresses, phone numbers, and positions. As she was leaving, she remembered that she had her personal USB flash drive in her purse. She decided the USB drive would be good to use in case she had an attachment problem with the email she had already sent. Although much of the USB drive's space was taken up with family photos she had shared with her coworkers earlier in the day, there was still enough room to add the data extract. She copied the data extract and dropped it in her purse as she left for her appointment. When she arrived home that evening, she plugged the USB drive into her family's computer and used her spreadsheet application to analyze the data.

The following are additional questions for this scenario:

1. Which data elements contained in this data extract should be considered PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

3. What privacy-specific safeguards might help protect the PII contained in the data extract?

4. What should the employee do if her purse (containing the USB drive) is stolen? What should the organization do? How could the employer have prevented this situation?

5. What should the employee do with the copies of the extract when she finishes her work?

6. Should the emailing of the extract to a personal email address be considered a breach? Should storing the data on the personal USB drive be considered a breach?

7. What could the organization do to reduce the likelihood of similar events in the future?

8. How should this scenario be handled if the information is a list of de-identified retirement income statistics? Would the previous questions be answered differently?

Scenario 4: Testing Systems

An organization needed to test an upgrade to its fingerprint matching system before the upgrade could be introduced into the production environment. Because it is difficult to simulate fingerprint image and template data, the organization used real biometric image and template data to test the system. In addition to the fingerprint images and templates, the system also processed the demographic data associated with each fingerprint image, including name, age, sex, race, date of birth, and nationality. After successful completion of the testing, the organization upgraded its production system.

1. Which data elements contained in this system test should be considered PII?

2. What is the PII confidentiality impact level? What factors were taken into consideration when making this determination?

3. What privacy-specific safeguards might help protect the PII used in this test?

4. Is a PIA required to conduct this testing? Is a PIA required to complete the production system upgrade?

5. What should the organization do with the data used for testing when it completes the upgrade?

Appendix B—Frequently Asked Questions (FAQ)

Privacy and security leadership and staff, as well as others, may have questions about identifying, handling, and protecting the confidentiality of personally identifiable information (PII). This appendix contains frequently asked questions (FAQ) related to PII. Organizations are encouraged to customize this FAQ and make it available to their user community.

1. **What is personally identifiable information (PII)?**

   PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[81]

2. **What are examples of PII**?

   The following examples are meant to offer a cross-section of the types of information that could be considered PII, either singly or collectively, and is not an exhaustive list of all possibilities. Examples of PII include financial transactions, medical history, criminal history, employment history, individual's name, social security number, passport number, driver's license number, credit card number, vehicle registration, x-ray, patient ID number, and biometric data (e.g., retina scan, voice signature, facial geometry).[82]

3. **Does the definition of *individual* apply to foreign nationals?**

   OMB defined the term *individual*, as used in the definition of PII, to mean a citizen of the United States or an alien lawfully admitted for permanent residence, which is based on the Privacy Act definition.[83] For the purpose of protecting the confidentiality of PII, organizations may choose to administratively expand the scope of application to foreign nationals without creating new legal rights. Expanding the scope may reduce administrative burdens and improve operational efficiencies in the protection of data by eliminating the need to maintain separate systems or otherwise separate data. Additionally, the status of citizen, alien, or legal permanent resident can change over time, which makes it difficult to accurately identify and separate the data of foreign nationals. Expanding the scope may also serve additional organizational interests, such as providing reciprocity for data sharing agreements with other organizations.

   Agencies may also, consistent with individual practice, choose to extend the protections of the Privacy Act to foreign nationals without creating new judicially enforceable legal rights. For example, DHS has chosen to extend Privacy Act protections (e.g., access, correction) to foreign

[81] GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008, http://www.gao.gov/new.items/d08536.pdf.

[82] Organizations may want to consider how PII relating to deceased individuals should be handled, such as continuing to protect its confidentiality or properly destroying the information. Organizations may want to base their considerations on any obligations to protect, organizational policies, or evaluation of organization-specific risk factors. With respect to organization-specific risk factors, there is a balancing act because PII relating to deceased individuals can both promote and prevent identity theft. For example, making available lists of deceased individuals can prevent some types of fraud, such as voter fraud. In contrast, PII of a deceased individual also could be used to open a credit card account or to set up a false cover for criminals. Organizations should consult with their legal counsel and privacy officer.

[83] OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, http://www.whitehouse.gov/omb/memoranda/m03-22.html#1.

nationals whose data resides in mixed systems, which are systems of records with information about both U.S. persons and non-U.S. persons.[84]

Organizations should consult with legal counsel to determine if they have an additional obligation to protect the confidentiality of the personal information relating to foreign nationals, such as the Immigration and Nationality Act, which requires the protection of the confidentiality of Visa applicant data.[85]

4. How did the need for guidelines on protecting PII come about? Why is this important?

With the increased use of computers for the processing and dissemination of data, the protection of PII has become more important to maintain public trust and confidence in an organization, to protect the reputation of an organization, and to protect against legal liability for an organization. Recently, organizations have become more concerned about the risk of legal liability due to the enactment of many federal, state, and international privacy laws, as well as the increased opportunities for misuse that accompany the increased processing and dissemination of PII.

In the United States, Federal privacy laws are generally sector-based. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to the health care sector, and the Gramm-Leach-Bliley Act of 1999 (GLBA) applies to the financial services sector. In contrast, many states have enacted their own generally applicable privacy laws, such as breach notification laws. Some U.S.-based organizations that conduct business abroad must also comply with international privacy laws, which vary greatly from country to country. Organizations are responsible for determining which laws apply to them based on sector and jurisdiction.

For Federal government agencies, the need to protect PII was first established by the Privacy Act of 1974. It required Federal agencies to protect PII and apply the Fair Information Practices to PII. Also, the Privacy Act required agencies to "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

In response to the increased use of computers and the Internet to process government information, the E-Government Act of 2002 was enacted to ensure public trust in electronic government services. It required Federal agencies to conduct Privacy Impact Assessments (PIAs) and to maintain privacy policies on their web sites. The E-Government Act also directed OMB to issue implementation guidance to Federal agencies. In 2003, OMB issued M-03-22 to provide guidance on PIAs and web site privacy policies. OMB has continued to provide privacy guidance to Federal agencies on many PII protection topics such as remote access to PII, encryption of PII on mobile devices, and breach notification (see Appendix G for additional information).

Additionally, Federal agencies are required to comply with other privacy laws, such as the Children's Online Privacy Protection Act (COPPA) and HIPAA (only if the agency acts as a health care provider or other covered entity as defined by the statute).

[84] See *DHS Privacy Policy Regarding Collection, Use Retention, and Dissemination of Information on Non-U.S. Persons*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.

[85] Immigration and Nationality Act, 8 U.S.C. § 1202.

5. What is the Privacy Act?

The Privacy Act of 1974 is the foundation of public sector privacy law in the U.S. It applies only to Federal agencies and provides a statutory basis for the required use of Fair Information Practices. The Privacy Act pertains only to data maintained within a System of Records (SOR), which means any "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[86] Record is defined broadly to include any item of information about an individual, both paper and electronic.

The basic provisions of the Privacy Act include the following:

- Provide notice to individuals that explains:[87]
  - The authority for the data collection
  - The purpose of the data collection
  - Routine uses for the data
  - Effects, if any, of not providing the information
- Limit collection of data to the minimum necessary to accomplish the purpose of the agency
- Collect information directly from the person about whom the information pertains, if possible
- Maintain accuracy and completeness of the data
- Disclose the data to only those who need access for proper purposes, such as sharing for an identified routine use or to perform agency work
- Allow individuals to access data pertaining to them, request correction of wrong or incomplete data, and make an appeal for denials of requests for access and correction
- Maintain appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of the records.

Violations of the Privacy Act can result in civil and criminal liability.

Most information contained within a Privacy Act SOR is considered to be PII, but not all PII is contained within a Privacy Act SOR. Organizations that seek to protect systems (e.g., via security controls) containing PII may be able to realize efficiencies by coordinating with efforts to comply with the Privacy Act, as these activities will often be similar.

6. What is a Privacy Impact Assessment (PIA)? When do I need to conduct a PIA?

The E-Government Act of 2002 required Federal agencies to conduct PIAs, which are processes for identifying and mitigating privacy risks within an information system. PIAs should address risk at every stage of the system development life cycle (SDLC). Most organizations have established their

[86] 5 U.S.C. § 552a (a)(5).

[87] The Privacy Act also requires publication of general notice in the Federal Register, which is called a System of Records Notice (SORN).

own templates that provide the basis for conducting a PIA. The E-Government Act of 2002 requires Federal agencies to conduct PIAs when:

- Developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
- Initiating a new collection of information that—
  - Will be collected, maintained, or disseminated using information technology; and
  - Includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

The E-Government Act authorized OMB to provide Federal agencies with guidance on conducting PIAs, which resulted in OMB Memorandum 03-22. The Memorandum provided examples of system changes that create new privacy risks and trigger the requirement for a new PIA:

- **Conversions**—when paper-based records are to be converted to electronic systems
- **De-Identified to Identifiable**—when functions applied to an existing information collection change de-identified information into information in identifiable form
- **Significant System Management Changes**—when new uses of an existing information system, including application of new technologies, significantly change how information in identifiable form is managed in the system
- **Significant Merging**—when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated
- **New Public Access**—when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an information system accessed by members of the public
- **Commercial Sources**—when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources
- **New Interagency Uses**—when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives
- **Internal Flow or Collection**—when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form
- **Alteration in Character of Data**—when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)

The E-Government Act requires publication of PIAs,[88] which must analyze and describe the following information:

- What information is to be collected
- Why the information is being collected
- The intended use of the information
- With whom the information will be shared
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent
- How the information will be secured
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a
- What choices the agency made regarding an information system or collection of information as a result of performing the PIA.

7. What is the Paperwork Reduction Act?

The Paperwork Reduction Act (PRA) gives OMB and other Federal agencies responsibilities for the management of information resources.[89] The PRA is relevant to PII protection for two major reasons. First, it places privacy among the responsibilities of agency CIOs. However, the extent to which agency CIOs are responsible for privacy depends on a number of factors, including whether the agency is covered by any other statutory mandate for the designation of a chief privacy officer (CPO).[90] Second, the PRA created a process for OMB review and approval of Federal agency information collections from the public. This process is relevant to PII protection because it provides a mechanism for agencies to limit the collection of PII, as mandated by the Fair Information Practice of Collection Limitation. It is also relevant to PII protection because its terms partly define the scope of E-Government Act PIAs. The purpose of the PRA information collection review process is to minimize the burdens of paperwork on the public, minimize the cost of information collections, and increase the quality of Federal information.[91] The PRA requires Federal agencies to get clearance from OMB when an agency plans to collect information from ten or more persons using identical reporting, recordkeeping, or disclosure requirements. The term *persons* is defined broadly to include people, organizations, local government, etc., but it does not include Federal agencies or employees of Federal agencies when acting in their official capacities. Agencies must also provide notice of the collection in the Federal Register before submitting the information collection to OMB for clearance.

[88] An agency may exempt itself from this requirement if publication of the PIA would raise national security concerns or reveal classified or sensitive information.

[89] The PRA is codified at 44 U.S.C. § 3501, et seq. First enacted into law in 1980 (Pub. L. 96-511, Dec. 11, 1980), the PRA was significantly amended in 1995 (Pub. L. 104-13, May 22, 1995). The Clinger-Cohen Act of 1996 amended the PRA to make agency Chief Information Officers (CIO) responsible for carrying out agency responsibilities under the Act (sec. 5125(a), Pub. L. 104-106, 110 Stat. 684, Feb. 10, 1996).

[90] For example, chief (or senior) privacy officers are required by the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act of 2005, for the agencies covered by that Act (sec. 522, Div. H, Pub. L. 108-447, Dec. 8, 2004), for the Department of Homeland Security by sec. 222, Homeland Security Act, Pub. L. 107-296, Nov. 25, 2002 (6 U.S.C. § 142), and for the Department of Justice by sec. 1174, Violence Against Women and Dept. of Justice Reauthorization Act of 2005, Pub. L. 109-162, Jan. 5, 2006 (28 U.S.C. § 509).

[91] For additional information, see: http://ocio.os.doc.gov/ITPolicyandPrograms/Information_Collection/dev01_003742.

OMB reviews the proposed information collection and assigns a control number to the collection, which must be displayed on the collection form.

8. What are the general risks to individuals and the organization if PII is misused?

Depending on the type of information lost, an individual may suffer social, economic, or physical harm. If the information lost is sufficient to be exploited by an identity thief, the person can suffer, for example, from a loss of money, damage to credit, a compromise of medical records, threats, and/or harassment. The individual may suffer tremendous losses of time and money to address the damage. Other types of harm that may occur to individuals include denial of government benefits, blackmail, discrimination, and physical harm.

Organizations also face risks to their finances and reputation. If PII is misused, organizations may suffer financial losses in compensating the individuals, assisting them in monitoring their credit ratings, and addressing administrative concerns. In addition, recovering from a major breach is costly to many organizations in terms of time spent by key staff in coordinating and executing appropriate responses. If a loss of PII constitutes a violation of relevant law, the organization and/or its staff may be subject to criminal or civil penalties, or it may have to agree to receive close government scrutiny and oversight. Another major risk to organizations is that their public reputation and public confidence may be lost, potentially jeopardizing the organizations' ability to achieve their missions.

9. What should I consider when reviewing restrictions on collecting PII?

Key considerations to review are any legal requirements that could impact PII collections. One should ask what laws, regulations, and guidance are applicable to the organization considering the type of PII that is collected (e.g., Privacy Act, Paperwork Reduction Act, and the E-Government Act for general PII; HIPAA for health PII; GLBA for financial PII; COPPA for children's PII). An organization's legal counsel and privacy officer should always be consulted to determine whether there are restrictions on collecting PII.

Consistent with the Fair Information Practices of Collection Limitation and Use Limitation, one could more specifically ask if the collected PII is absolutely necessary to do business (i.e., does it support the business purpose of the system or the organization's mission?). If it does not serve a viable business purpose, then Federal agencies may not collect that PII. If the collection of PII does serve a business purpose, then it should be collected, used, shared, and disseminated appropriately.

10. What is different about protecting PII compared to any other data, and how should PII be protected?

In many cases, protection of PII is similar to protection of other data and includes protecting the confidentiality, integrity, and availability of the information. Most security controls used for other types of data are also applicable to the protection of PII. For PII, there are several privacy-specific safeguards, such as anonymization, minimization of PII collection, and de-identification.

In addition to protection requirements for PII, there are other requirements for the handling of PII. The Fair Information Practices provide best practice guidelines, such as Purpose Specification, Use Limitation, Accountability, and Data Quality. Moreover, the factors for assigning a confidentiality impact level to PII are different than other types of data. Breaches to the confidentiality of PII harm both the organization and the individual. Harm to individuals should be factored in strongly because of the magnitude of the potential harm, such as identity theft, embarrassment, and denial of benefits.

Appendix C—Other Terms and Definitions for Personal Information

Laws, regulations, and guidance documents provide various terms and definitions used to describe personal information, such as *information in identifiable form* (IIF), *system of records* (SOR), and *protected health information* (PHI). Some of these are similar to the definition of PII used in this document. However, organizations should not use the term PII (as defined in this document) interchangeably with these terms and definitions because they are specific to their particular context. The table below provides examples of these other terms and definitions, and it is not intended to be comprehensive.

Defining Authority	Term	Definition	Comments
E-Government Act of 2002, Pub. L.107-347, 116 Stat. 2899, see § 208(d).	Information in Identifiable Form (IIF)	Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.	Often considered to have been replaced by the term PII.
OMB Memorandum 03-22	Information in Identifiable Form (IIF)	Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)	Often considered to have been replaced by the term PII.
OMB Memorandum 03-22	Individual	A citizen of the United States or an alien lawfully admitted for permanent residence.	This definition mirrors the Privacy Act definition.
OMB Memorandum 06-19	Personally Identifiable Information (PII)	Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.	
OMB Memorandum 07-16	Personally Identifiable Information (PII)	Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.	

Defining Authority	Term	Definition	Comments
Health Insurance Portability and Accountability Act of 1996 (HIPAA), ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS, 45 C.F.R. § 160.103.	Individually Identifiable Health Information (IIHI)	Information that is a subset of health information, including demographic information collected from an individual, and: - Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and - Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and - That identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.	Applicable only to the HIPAA; subject to a number of exemptions not made for PII.
Health Insurance Portability and Accountability Act of 1996 (HIPAA), ADMINISTRATIVE DATA STANDARDS AND RELATED REQUIREMENTS, 45 C.F.R. § 160.103.	Protected Health Information (PHI)	Individually identifiable health information (IIHI) that is: - Transmitted by electronic media; - Maintained in electronic media; or - Transmitted or maintained in any other form or medium. Protected health information excludes individually identifiable health information in: - Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; - Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and - Employment records held by a covered entity in its role as employer.	Applicable only to the HIPAA; subject to a number of exemptions not made for PII.
Privacy Act of 1974, 5 U.S.C. § 552a(a)(5).	System of Records (SOR)	A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.	Applies only to Federal agencies. Provides some exemptions for certain types of records.
Privacy Act of 1974, 5 U.S.C. § 552a(a)(2).	Individual	A citizen of the United States or an alien lawfully admitted for permanent residence.	

Defining Authority	Term	Definition	Comments
Privacy Act of 1974, 5 U.S.C. § 552a(a)(4).	Record	Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.	

Defining Authority	Term	Definition	Comments
Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (a)(4).	Education Records	Records, files, documents, and other materials which: - contain information directly related to a student; and - are maintained by an educational agency or institution or by a person acting for such agency or institution, subject to some exceptions. Exceptions include: - records of instructional, supervisory, and administrative personnel and educational personnel ancillary thereto which are in the sole possession of the maker thereof and which are not accessible or revealed to any other person except a substitute; - records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement; - in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or - records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.	Applies only to educational institutions receiving funds from the Federal government.

Appendix D—Fair Information Practices

The Fair Information Practices, also known as Privacy Principles, are the framework for most modern privacy laws around the world. Several versions of the Fair Information Practices have been developed through government studies, Federal agencies, and international organizations. These different versions share common elements, but the elements are divided and expressed differently. The most commonly used versions are discussed in this appendix.[92]

In 1973, the U.S. Department of Health, Education, and Welfare (HEW) (now the Department of Health and Human Services) issued a report entitled *Records, Computers, and the Rights of Citizens* (commonly referred to as the *HEW Report*). The report was the culmination of an extensive study into data processing in the public and private sectors. The HEW Report recommended that Congress enact legislation adopting a "Code of Fair Information Practices" for automated personal data systems. The recommended Fair Information Practices became the foundation for the Privacy Act of 1974. The HEW Report Fair Information Practices included the following:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information is in his or her file and how the information is being used.
- There must be a way for an individual to correct information in his or her records.
- Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse.
- There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

In 1980, the Organisation for Economic Co-operation and Development (OECD)[93] adopted *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, which provide a framework for privacy that has been referenced in U.S. Federal guidance and internationally. The OECD Guidelines, along with the Council of Europe Convention,[94] became the foundation for the European Union's Data Protection Directive.[95] The OECD Guidelines include the following Privacy Principles:

- **Collection Limitation—**There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data Quality—**Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[92] Portions of this appendix were contributed to and published in the Executive Office of the President, National Science and Technology Council's *Identity Management Task Force Report 2008*, see http://www.ostp.gov/galleries/NSTC%20Reports/IdMReport%20Final.pdf.

[93] The U.S. is an OECD member country and participated in the development of the OECD Privacy Guidelines, see http://www.ftc.gov/speeches/thompson/thomtacdremarks.shtm.

[94] In 1981, the Council of Europe enacted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, which also recognized the Fair Information Practices.

[95] In 1995, the European Union enacted the *Data Protection Directive*, Directive 95/46/EC, which required member states to harmonize their national legislation with the terms of the Directive, including the Fair Information Practices. For additional information, see Jody R. Westby, *International Guide to Privacy*, American Bar Association Publishing, 2004.

- **Purpose Specification—**The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **Use Limitation—**Personal data should not be disclosed, made available or otherwise used for purposes other than those specified, except with the consent of the data subject or by the authority of law.
- **Security Safeguards—**Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
- **Openness—**There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
- **Individual Participation**—An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.
- **Accountability—**A data controller should be accountable for complying with measures which give effect to the principles stated above.

In 2004, the Federal CIO Council published the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP).[96] It included a set of privacy control families based on Fair Information Practices. The privacy control families were intended to provide guidance for integrating privacy requirements into the Federal Enterprise Architecture. In 2009, the CIO Council drafted a revised set of privacy control families.[97] The revised set contains the following privacy control families:

- **Transparency**—Providing notice to the individual regarding the collection, use, dissemination, and maintenance of PII.
- **Individual Participation and Redress**—Involving the individual in the process of using PII and seeking individual consent for the collection, use, dissemination, and maintenance of PII. Providing mechanisms for appropriate access, correction, and redress regarding the use of PII.
- **Purpose Specification**— Specifically articulating the authority that permits the collection of PII and specifically articulating the purpose or purposes for which the PII is intended to be used.
- **Data Minimization and Retention**—Only collecting PII that is directly relevant and necessary to accomplish the specified purpose(s). Only retaining PII for as long as is necessary to fulfill the specified purpose(s) and in accordance with the National Archives and Records Administration (NARA) approved record retention schedule.

[96] FEA-SPP, Version 2, http://cio.gov/documents/Security_and_Privacy_Profile_v2.pdf.

[97] This set of privacy control families is based on the working draft of Version 3 of FEA-SPP, August 28, 2009. It is expected to be finalized and published in 2010.

- **Use Limitation**—Using PII solely for the purpose(s) specified in the public notice. Sharing information should be for a purpose compatible with the purpose for which the information was collected.
- **Data Quality and Integrity**—Ensuring, to the greatest extent possible, that PII is accurate, relevant, timely, and complete for the purposes for which it is to be used, as identified in the public notice.
- **Security**—Protecting PII (in all media) through appropriate administrative, technical, and physical security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
- **Accountability and Auditing**—Providing accountability for compliance with all applicable privacy protection requirements, including all identified authorities and established policies and procedures that govern the collection, use, dissemination, and maintenance of PII. Auditing for the actual use of PII to demonstrate compliance with established privacy controls.

In 2004, the Asia-Pacific Economic Cooperation (APEC) ministers officially endorsed the Privacy Framework[98] developed within one of its committees. The APEC Privacy Framework was based on the OECD Privacy Guidelines and was developed to encourage electronic commerce among the member states and to build trust with the international community. The Privacy Framework includes the following Privacy Principles:

- **Preventing Harm—**Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.
- **Notice—**Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information.
- **Collection Limitation—**The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.
- **Uses of Personal Information—**Personal information collected should be used only to fulfill the purposes of the collection and other compatible related purposes, except with the consent of the individual, when necessary to provide a product or service requested by the individual, or by authority of law.
- **Choice—**Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.
- **Integrity of Personal Information—**Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
- **Security Safeguards—**Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other

[98] http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held, and they should be subject to periodic review and reassessment.

- **Access and Correction**—Individuals should be able to obtain from the personal information controller confirmation of whether the personal information controller holds personal information about them, have the information provided to them at a reasonable charge and within a reasonable time, and challenge the accuracy of the information, as well as have the information corrected or deleted. Exceptions include situations where the burden would be disproportionate to the risks to the individual's privacy, the information should not be disclosed due to legal or security concerns, and the privacy of other persons would be violated.
- **Accountability—**A personal information controller should be accountable for complying with measures that give effect to the Principles stated above.

Appendix E—Glossary

Selected terms used in the publication are defined below.

Aggregated Information: Information elements collated on a number of individuals, typically used for the purposes of making comparisons or identifying patterns.

Anonymized Information: Previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists.

Confidentiality: **"**Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information."[99]

Context of Use: The purpose for which PII is collected, stored, used, processed, disclosed, or disseminated.

De-identified Information: Records that have had enough PII removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.

Distinguishable Information: Information that can be used to identify an individual.

Harm: Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached.

Linkable Information: Information about or related to an individual for which there is a possibility of logical association with other information about the individual.

Linked Information: Information about or related to an individual that is logically associated with other information about the individual.

Obscured Data: Data that has been distorted by cryptographic or other means to hide information. It is also referred to as being masked or obfuscated.

Personally Identifiable Information (PII): "Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[100]

PII Confidentiality Impact Level: The PII confidentiality impact level—*low, moderate, or high*—indicates the potential harm that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

Privacy Impact Assessment (PIA): **"**An analysis of how information is handled that ensures handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; determines the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic

[99] 44 U.S.C. § 3542, http://uscode.house.gov/download/pls/44C35.txt.

[100] GAO Report 08-536, *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008, http://www.gao.gov/new.items/d08536.pdf.

information system; and examines and evaluates protections and alternative processes for handling information to mitigate potential privacy risks."[101]

System of Records: **"**A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[102]

Traceable: Information that is sufficient to make a determination about a specific aspect of an individual's activities or status.

[101] OMB M-03-22.

[102] The Privacy Act of 1974, 5 U.S.C. § 552a(a)(5).

Appendix F—Acronyms and Abbreviations

Selected acronyms and abbreviations used in the publication are defined below.

APEC	Asia-Pacific Economic Cooperation
CD	Compact Disc
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CIPSEA	Confidential Information Protection and Statistical Efficiency Act
COPPA	Children’s Online Privacy Protection Act
CPO	Chief Privacy Officer
DHS	U.S. Department of Homeland Security
FAQ	Frequently Asked Questions
FEA-SPP	Federal Enterprise Architecture Security and Privacy Profile
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GLBA	Gramm-Leach-Bliley Act
GRS	General Record Schedule
HEW	U.S. Department of Health, Education, and Welfare
HIPAA	Health Insurance Portability and Accountability Act
ID	Identification
IIF	Information in Identifiable Form
IIHI	Individually Identifiable Health Information
IP	Internet Protocol
IPA	Initial Privacy Assessment
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
IT	Information Technology
ITL	Information Technology Laboratory
MAC	Media Access Control
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NPPI	Non-Public Personal Information
OECD	Organisation for Economic Co-operation and Development
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PDA	Personal Digital Assistant
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

PRA	Paperwork Reduction Act
PTA	Privacy Threshold Analysis
SDLC	System Development Life Cycle
SOR	System of Records
SORN	System of Records Notice
SP	Special Publication
SSN	Social Security Number
URL	Uniform Resource Locator
USB	Universal Serial Bus
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

Appendix G—Resources

Personnel involved with protecting PII and concerned about individual and organizational impact may want to review the following privacy laws and requirements that apply to Federal agencies.[103] Additionally, OMB has issued several memoranda that provide policy guidance and instructions for the implementation of privacy requirements.

Document	URL
Children's Online Privacy Protection Act (COPPA)	http://www.ftc.gov/ogc/coppa1.htm
Confidential Information Protection and Statistical Efficiency Act (CIPSEA)[104]	http://www.whitehouse.gov/omb/inforeg/cipsea/cipsea_statute.pdf
Confidential Information Protection and Statistical Efficiency Act (CIPSEA) Implementation Guidance	http://www.whitehouse.gov/omb/fedreg/2007/061507_cipsea_guidance.pdf
Consolidated Appropriations Act of 2005, Section 522	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_bills&docid=f:h4818enr.txt.pdf
E-Government Act of 2002, Section 208	http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.2458.ENR:
Federal Information Security Management Act (FISMA)[105]	http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
Identity Theft and Assumption Deterrence Act of 1998	http://www.ftc.gov/os/statutes/itada/itadact.htm
Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.)	http://caselaw.lp.findlaw.com/casecode/uscodes/50/chapters/15/subchapters/iv/sections/section_421.html
FIPS 140-2, *Security Requirements for Cryptographic Modules*	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
Freedom of Information Act (FOIA)[106]	http://www.justice.gov/oip/amended-foia-redlined.pdf
Gramm-Leach-Bliley Act (GLBA)	http://thomas.loc.gov/cgi-bin/query/z?c106:S.900.ENR:
Health Insurance Portability and Accountability Act (HIPAA)	http://aspe.hhs.gov/admnsimp/pl104191.htm
Implementing Recommendations of the 9/11 Commission Act of 2007	http://www.govtrack.us/congress/bill.xpd?bill=h110-1
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf
NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf

[103] This list is provided for reference only and is not an exhaustive list. For additional information, an organization's legal counsel and privacy officer should be consulted.

[104] CIPSEA is Title V of the E-Government Act of 2002.

[105] FISMA is Title III of the E-Government Act of 2002.

[106] FOIA was recently amended by the *OPEN Government Act of 2007*, Pub. L. 110-175, 121 Stat. 2524 (2007).

Document	URL
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Organizations and Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf
NIST SP 800-60 Revision 1, *Volume 1: Guide for Mapping Types of Information and Information Systems to Security Categories*	http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*	http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
NIST SP 800-63 Version 1.0.2, *Electronic Authentication Guidelines*[107]	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response*	http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf
NIST SP 800-88, *Guidelines for Media Sanitization*	http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf
Office of Personnel Management (OPM), *Guidance on Protecting Federal Employee Social Security Numbers and Combating Identity Theft*, June 2007	http://www.chcoc.gov/Transmittals/TransmittalDetails.aspx?TransmittalID=847
OMB Circular A-130, *Management of Federal Information Resources*	http://www.whitehouse.gov/omb/circulars/a130/a130.html
OMB Memorandum M-01-05, *Guidance on Inter-agency Sharing of Personal Data – Protecting Personal Privacy*	http://www.whitehouse.gov/omb/memoranda/m01-05.html
OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*	http://www.whitehouse.gov/omb/memoranda/m03-22.html
OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*	http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
OMB Memorandum M-05-08, *Designation of Senior Agency Officials for Privacy*	http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf
OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*	http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf
OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*	http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf
OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*	http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-19.pdf
OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*	http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

[107] NIST SP 800-63-1 was released as a draft in December 2008, http://csrc.nist.gov/publications/drafts/800-63-rev1/SP800-63-Rev1_Dec2008.pdf.

Document	URL
OMB Memorandum, September 20, 2006, *Recommendations for Identity Theft Related Data Breach Notification*	http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf
OMB Memorandum, July 2007, *Common Risks Impeding the Adequate Protection of Government Information* (developed jointly with DHS)	http://www.whitehouse.gov/omb/pubpress/2007/071707_best_practices.pdf
Paperwork Reduction Act	http://www.archives.gov/federal-register/laws/paperwork-reduction/
President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan*, April 2007	http://www.idtheft.gov/reports/StrategicPlan.pdf
Privacy Act of 1974	http://www.justice.gov/opcl/privstat.htm
Sensitive Database Extracts Technical Frequently Asked Questions	http://csrc.nist.gov/drivers/documents/OMB/OMB-M-07-16-Data-Extract-FAQ.pdf

NIST Special Publication 800-60 Volume I
Revision 1

National Institute of
Standards and Technology
U.S. Department of Commerce

Volume I:
Guide for Mapping Types of Information and Information Systems to Security Categories

Kevin Stine
Rich Kissel
William C. Barker
Jim Fahlsing
Jessica Gulick

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2008

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND
TECHNOLOGY
James M. Turner, Deputy Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof-of-concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. This Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government, and academic organizations.

Authority

This document has been developed by the National Institute of Standards and Technology (NIST) to further its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by federal agencies. It may also be used by nongovernmental organizations on a voluntary basis and is not subject to copyright. (Attribution would be appreciated by NIST.)

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

NIST Special Publication 800-60 Volume I, Revision 1, 53 pages

(Date) CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There are references in this publication to documents currently under development by NIST in accordance with responsibilities assigned to NIST under the Federal Information Security Management Act of 2002. The methodologies in this document may be used even before the completion of such companion documents. Thus, until such time as each document is completed, current requirements, guidelines, and procedures (where they exist) remain operative. For planning and transition purposes, agencies may wish to closely follow the development of these new documents by NIST. Individuals are also encouraged to review the public draft documents and offer their comments to NIST. All NIST documents mentioned in this publication, other than the ones noted above, are available at http://csrc.nist.gov/publications.

COMMENTS MAY BE SUBMITTED TO THE COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY
LABORATORY, NIST VIA ELECTRONIC MAIL AT SEC-CERT@NIST.GOV OR VIA REGULAR MAIL AT
100 BUREAU DRIVE (MAIL STOP 8930), GAITHERSBURG, MD 20899-8930

Acknowledgements

The authors, Kevin Stine, Rich Kissel, and William C. Barker, wish to thank their colleagues, Jim Fahlsing and Jessica Gulick from Science Applications International Corporation (SAIC), who helped update this document, prepare drafts, and review materials. In addition, special thanks are due to our reviewers, Arnold Johnson (NIST), Karen Quigg (Mitre Corporation), and Ruth Bandler (Food and Drug Administration), who greatly contributed to the document's development. A special note of thanks goes to Elizabeth Lennon for her superb technical editing and administrative support. NIST also gratefully acknowledges and appreciates the many contributions from individuals in the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories

Table of Contents

EXECUTIVE SUMMARY

Title III of the E-Government Act (Public Law 107-347), titled the Federal Information Security Management Act (FISMA), tasked the National Institute of Standards and Technology (NIST) to develop:

- Standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each such category; and
- Minimum information security requirements (i.e., management, operational, and technical security controls), for information and information systems in each such category.

In response to the second of these tasks, this guideline has been developed to assist Federal government agencies to categorize information and information systems. The guideline's objective is to facilitate application of appropriate levels of information security according to a range of levels of impact or consequences that might result from the unauthorized disclosure, modification, or use of the information or information system. This guideline assumes that the user is familiar with *Standards for Security Categorization of Federal Information and Information Systems* (Federal Information Processing Standard [FIPS] 199). The guideline and its appendices:

- Review the security categorization terms and definitions established by FIPS 199;
- Recommend a security categorization process;
- Describe a methodology for identifying types of Federal information and information systems;
- Suggest provisional[1] security impact levels for common information types;
- Discuss information attributes that may result in variances from the provisional impact level assignment; and
- Describe how to establish a system security categorization based on the system's use, connectivity, and aggregate information content.

This document is intended as a reference resource rather than as a tutorial and not all of the material will be relevant to all agencies. This document includes two volumes, a basic guideline and a volume of appendices. Users should review the guidelines provided in Volume I, then refer to only that specific material from the appendices that applies to their own systems and applications. The provisional impact assignments are provided in Volume II, Appendix C and D. The basis employed in this guideline for the identification of information types is the Office of

[1] Provisional security impact levels are the initial or conditional impact determinations made until all considerations are fully reviewed, analyzed, and accepted in the subsequent categorization steps by appropriate officials.

Management and Budget’s Federal Enterprise Architecture (FEA) Program Management Office (PMO) October 2007 publication, *The Consolidated Reference Model Document Version 2.3*.

1.0 INTRODUCTION

The identification of information processed on an information system is essential to the proper selection of security controls and ensuring the confidentiality, integrity, and availability of the system and its information. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 has been developed to assist Federal government agencies to categorize information and information systems.

1.1 Purpose and Applicability

NIST SP 800-60 addresses the FISMA direction to develop guidelines recommending the types of information and information systems to be included in each category of potential security impact. This guideline is intended to help agencies consistently map security impact levels to types of: (i) information (e.g., privacy, medical, proprietary, financial, contractor sensitive, trade secret, investigation); and (ii) information systems (e.g., mission critical, mission support, administrative). This guideline applies to all Federal information systems other than *national security systems*. *National security systems* store, process, or communicate *national security* information.[2]

1.2 Target Audience

This publication is intended to serve a diverse federal audience of information system and information security professionals including: (i) individuals with information system and information security management and oversight responsibilities (e.g., chief information officers, senior agency information security officers, authorizing officials); (ii) organizational officials having a vested interest in the accomplishment of organizational missions (e.g., mission and business area owners, information owners); (iii) individuals with information system development responsibilities (e.g., program and project managers, information system developers); and (iv) individuals with information security implementation and operational responsibilities (e.g., information system owners, information owners, information system security officers).

1.3 Relationship to Other Documents

NIST Special Publication (SP) 800-60 is a member of the NIST family of security-related publications including:

- FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems;*
- FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*;

[2] FISMA defines a *national security system* as any information system (including telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency – (i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a routine administrative or business system used for applications such as payroll, finance, logistics, and personnel management); or (ii) that processes classified information. [See Public Law 107-347, Section 3542 (b)(2)(A).]

- NIST SP 800-30, *Risk Management Guide for Information Technology Systems;*[3]
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems;*
- NIST Draft SP 800-39, *Managing Risk from Information Systems: An Organization Perspective;*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems;*
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; and
- NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*.

This series of nine documents is intended to provide a structured, yet flexible framework for selecting, specifying, employing, evaluating, and monitoring the security controls in Federal information systems—and thus, makes a significant contribution toward satisfying the requirements of the Federal Information Security Management Act (FISMA) of 2002. While the publications are mutually reinforcing and have some dependencies, in most cases, they can be effectively used independently of one another.

The SP 800-60 information types and associated security impact levels are based on the Office of Management and Budget (OMB) Federal Enterprise Architecture Program Management Office's October 2007 *FEA Consolidated Reference Model Document*, *Version 2.3*, inputs from participants in previous NIST SP 800-60 workshops, and FIPS 199. Rationale for the example impact-level recommendations provided in the appendices has been derived from multiple sources and, as such, will require several iterations of review, comment, and subsequent modification to achieve consistency in terminology, structure, and content.

1.4 Organization of this Special Publication

This is Volume I of two volumes. It contains the basic guidelines for mapping types of information and information systems to security categories. The appendices, including security categorization recommendations for mission-based information types and rationale for security categorization recommendations, are published as a separate Volume II.

Volume I provides the following background information and mapping guidelines:

- Section 2: Provides an overview of the value of the categorization process to agency missions, security programs and overall information technology (IT) management and the publication's role in the system development lifecycle, the certification and accreditation process, and the NIST Risk Management Framework.
- Section 3: Provides the security objectives and corresponding security impact levels identified in the Federal Information Processing Standard 199, *Standards for Security Categorization of Federal Information and Information Systems* [FIPS 199];

[3] This document is currently under revision and will be reissued as Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*.

- Section 4: Identifies the process including guidelines for identification of *mission-based* and *management and support* information types and the process used to select security impact levels, general considerations relating to security impact assignment, guidelines for system security categorization, and considerations and guidelines for applying and interrelating system categorization results to the agency’s enterprise, large supporting infrastructures, and interconnecting systems;
- Appendix A: Glossary; and
- Appendix B: References.

Volume II includes the following appendices:

- Appendix A: Glossary [Repeated];
- Appendix B: References [Repeated];
- Appendix C: Provisional security impact level assignments and supporting rationale for *management and support* information (administrative, management, and service information);
- Appendix D: Provisional security impact level assignments and supporting rationale for *mission-based* information (mission information and services delivery mechanisms); and
- Appendix E: Legislative and executive sources that specify sensitivity/criticality properties.

2.0 PUBLICATION OVERVIEW

Security categorization provides a vital step in integrating security into the government agency's business and information technology management functions and establishes the foundation for security standardization amongst their information systems. Security categorization starts with the identification of what information supports which government lines of business, as defined by the Federal Enterprise Architecture (FEA). Subsequent steps focus on the evaluation of the need for security in terms of confidentiality, integrity, and availability. The result is strong linkage between missions, information, and information systems with cost effective information security.

2.1 Agencies Support the Security Categorization Process

Agencies support the categorization process by establishing mission-based information types for the organization. The approach to establishing mission-based information types at an agency begins by documenting the agency's mission and business areas. In the case of mission-based information, the responsible individuals, in coordination with management, operational, enterprise architecture, and security stakeholders, should compile a comprehensive set of the agency's lines of business and mission areas. In addition, responsible individuals should identify the applicable sub-functions necessary to accomplish the organization's mission. For example, one organization's mission might be related to economic development. Sub-functions that are part of the organization's economic development mission might include business and industry development, intellectual property protection, or financial sector oversight. Each of these sub-functions represents an information type.

Agencies should conduct FIPS 199 security categorizations of their information systems as an agency-wide activity with the involvement of the senior leadership and other key officials within the organization (e.g., mission and business owners, authorizing officials, risk executive, chief information officer, senior agency information security officer, information system owners, and information owners) to ensure that each information system receives the appropriate management oversight and reflects the needs of the organization as a whole. Senior leadership oversight in the security categorization process is essential so that the next steps in the NIST Risk Management Framework[4] (e.g., security control selection) can be carried out in an effective and consistent manner throughout the agency.

2.2 Value to Agency Missions, Security Programs and IT Management

Federal agencies are heavily dependent upon information and information systems to successfully conduct critical missions. With an increasing reliability on and growing complexity of information systems as well as a constantly changing risk environment, information security has become a mission-essential function. This function must be conducted in a manner that reduces the risks to the information entrusted to the agency, its overall mission, and its ability to do business and to serve the American public. In the end, information security, as a function, becomes a business enabler through diligent and effective management of risk to information confidentiality, integrity, and availability.

[4] See Section 2.5, Figure 1: NIST Risk Management Framework

Therefore, the value of information security categorization is to enable agencies to proactively implement appropriate information security controls based on the assessed potential impact to information confidentiality, integrity, and availability and in turn to support their mission in a cost-effective manner. An incorrect information system impact analysis (i.e., incorrect FIPS 199 security categorization) can result in the agency either over protecting the information system thus wasting valuable security resources, or under protecting the information system and placing important operations and assets at risk. The aggregation of such mistakes at the enterprise level can further compound the problem.

In contrast, conducting FIPS 199 impact analyses as an agency-wide exercise with the participation of key officials (e.g., Chief Information Officer [CIO], Senior Agency Information Security Officer [SAISO], Authorizing Officials, Mission/System Owners) at multiple levels can enable the agency to leverage economies of scale through the effective management and implementation of security controls at the enterprise level. A resulting value of consistently implementing this systematic process for determining the security categorization and the application of appropriate security protection is an improved overall understanding of the agency's mission, business processes, and information and system ownership.

Implementation Tip

To enable an appropriate level of mission support and the diligent implementation of current and future information security requirements, each agency should establish a formal process to validate system level security categorizations in terms of agency priorities. This will not only promote comparable evaluation of systems, but also yield added benefits to include leveraging common security controls and establishing defense-in-depth.

2.3 Role in the System Development Lifecycle

An initial security categorization should occur early in the agency's system development lifecycle (SDLC). The resulting security categorization would feed into security requirements identification (later to evolve into security controls) and other related activities such as privacy impact analysis or critical infrastructure analysis. Ultimately, the identified security requirements and selected security controls are introduced to the standard systems engineering process to effectively integrate the security controls with the information systems functional and operational requirements, as well as other pertinent system requirements (e.g., reliability, maintainability, supportability).

2.4 Role in the Certification and Accreditation Process

Security categorization establishes the foundation of the certification and accreditation (C&A) activity by determining the levels of rigor required for certification and overall assurance testing of security controls, as well as additional activities that may be needed (i.e., privacy and critical infrastructure protection (CIP)). Thus, it assists in determining C&A level of effort and associated activity duration.

Security categorization is a prerequisite activity for the C&A process. The categorization should be revisited at least every three years or when significant change occurs to the system or supporting business lines. Situational changes outside the system or agency may require a reevaluation of the categorization (i.e., directed mission changes, changes in governance, elevated or targeted threat activities). For more information, see NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle* and NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

Implementation Tip

It is important to routinely revisit the security categorization as the mission/ business changes because it is likely the impact levels or even information types may change as well.

2.5 Role in the NIST Risk Management Framework

Security Categorization is the key first step in the Risk Management Framework[5] because of its effect on all other steps in the framework from selection of security controls to level of effort in assessing security control effectiveness.

Figure 1, NIST Risk Management Framework, depicts the role of NIST security standards and guidelines for information system security.

[5] NIST SP 800-39, *Managing Risk from Information Systems: An Organizational Perspective*, (Initial Public Draft), October 2007.

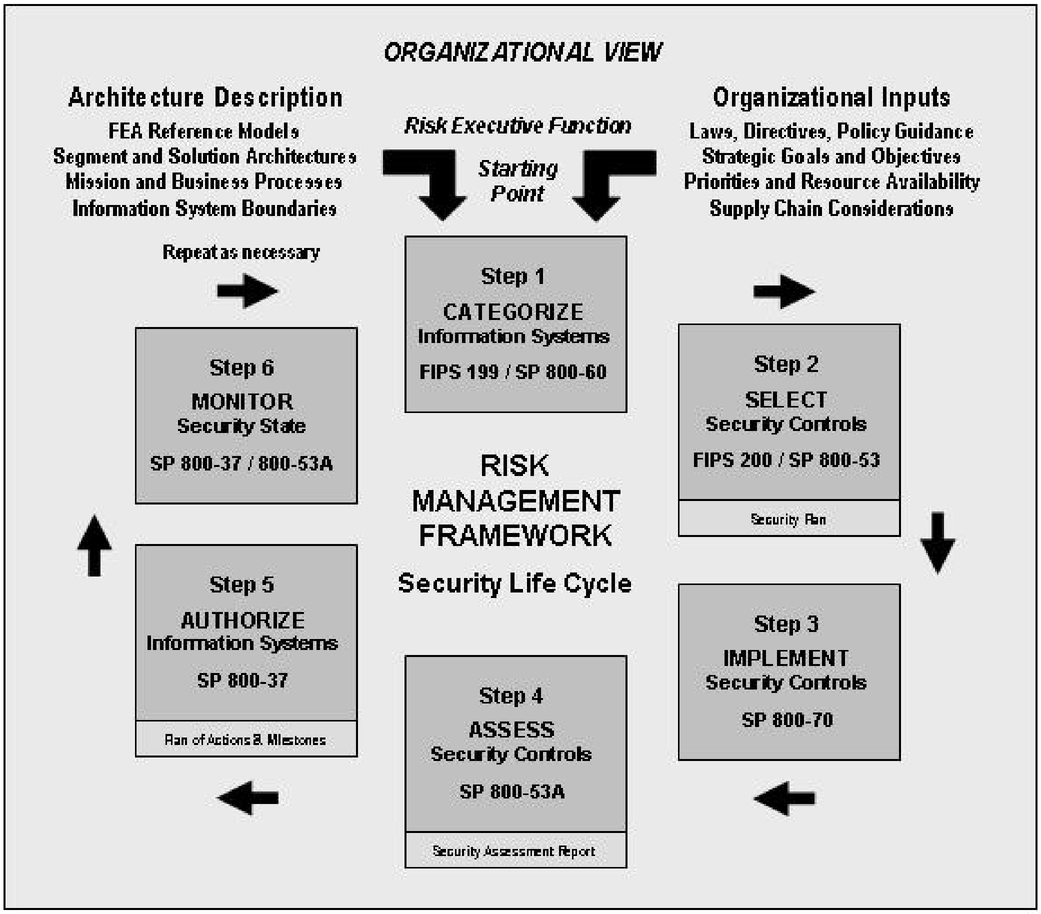


Figure 1: NIST Risk Management Framework

The security categorization process documented in this publication provides input into the following processes:

- Step 2: Select an initial set of security controls for the information system based on the FIPS 199 security categorization and apply tailoring guidance as appropriate, to obtain a starting point for required controls as specified in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems.* Utilizing NIST SP 800-53 and SP 800-30, *Risk Management Guide for Information Technology Systems, s*upplement the initial set of tailored security controls based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances.
- Step 3: Implement the security controls in the information system.
- Step 4: Assess the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. (Reference NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*).

- Step 5: Authorize information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable as specified in NIST SP 800-37*, Guide for the Security Certification and Accreditation of Federal Information Systems.*
- Step 6: Monitor and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis. (Reference NIST SP 800-37 and SP 800-53A).

3.0 Security Categorization of Information and Information Systems

Federal Information Processing Standard 199 (FIPS 199), *Standards for Security Categorization of Federal Information and Information Systems*, defines the security categories, security objectives, and impact levels to which SP 800-60 maps information types. FIPS 199 establishes security categories based on the magnitude of harm expected to result from compromises rather than on the results of an assessment that includes an attempt to determine the probability of compromise. FIPS 199 also describes the context of use for this guideline. Some of the content of FIPS 199 is included in this section in order to simplify the use of this guideline.

3.1 Security Categories and Objectives

3.1.1 Security Categories

FIPS 199 establishes security categories for both information[6] and information systems. The security categories are based on the potential impact on an organization should certain events occur. The potential impacts could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

FIPS 199 establishes three potential levels of impact (low, moderate, and high) relevant to securing Federal information and information systems for each of three stated security objectives (confidentiality, integrity, and availability).

3.1.2 Security Objectives and Types of Potential Losses

As reflected in Table 1, FISMA and FIPS 199 define three security objectives for information and information systems.

Table 1: Information and Information System Security Objectives

Security Objectives	FISMA Definition [44 U.S.C., Sec. 3542]	FIPS 199 Definition
Confidentiality	"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"	A loss of *confidentiality* is the unauthorized disclosure of information.
Integrity	"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…"	A loss of *integrity* is the unauthorized modification or destruction of information.
Availability	"Ensuring timely and reliable access to and use of information…"	A loss of *availability* is the disruption of access to or use of information or an information system.

[6] Information is categorized according to its *information type*. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

3.2 Impact Assessment

FIPS 199 defines three levels of *potential impact* on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The application of these definitions must take place within the context of each organization and the overall national interest. Table 2 provides FIPS 199 potential impact definitions.

Table 2: Potential Impact Levels

Potential Impact	Definitions
Low	The potential impact is **low** if—The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.[7] A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The potential impact is **moderate** if—The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is **high** if—The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

In FIPS 199, the security category of an information type can be associated with both user information and system information[8] and can be applicable to information in either electronic or non-electronic form. It is also used as input in considering the appropriate security category for a system. Establishing an appropriate security category for an information type simply requires determining the *potential impact* for each security objective associated with the particular information type. The generalized format for expressing the security category, or *SC*, of an information type is:

[7] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

[8] System information (e.g., network routing tables, password files, cryptographic key management information) must be protected at a level commensurate with the most critical or sensitive user information being processed by the information system to ensure confidentiality, integrity, and availability.

Security Category $_{\text{information type}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)}

where the acceptable values for potential *impact* are low, moderate, high, or not applicable.[9]

[9] The potential impact value of *not applicable* may be applied only to the confidentiality security objective.

4.0 ASSIGNMENT OF IMPACT LEVELS AND SECURITY CATEGORIZATION

This section provides a methodology for assigning security impact levels and security categorizations for information types and information systems consistent with the organization's assigned mission and business functions based on FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. This document assumes that the user has read and is familiar with FIPS 199. Figure 2 illustrates the four-step security categorization process and how it drives the selection of baseline security controls.

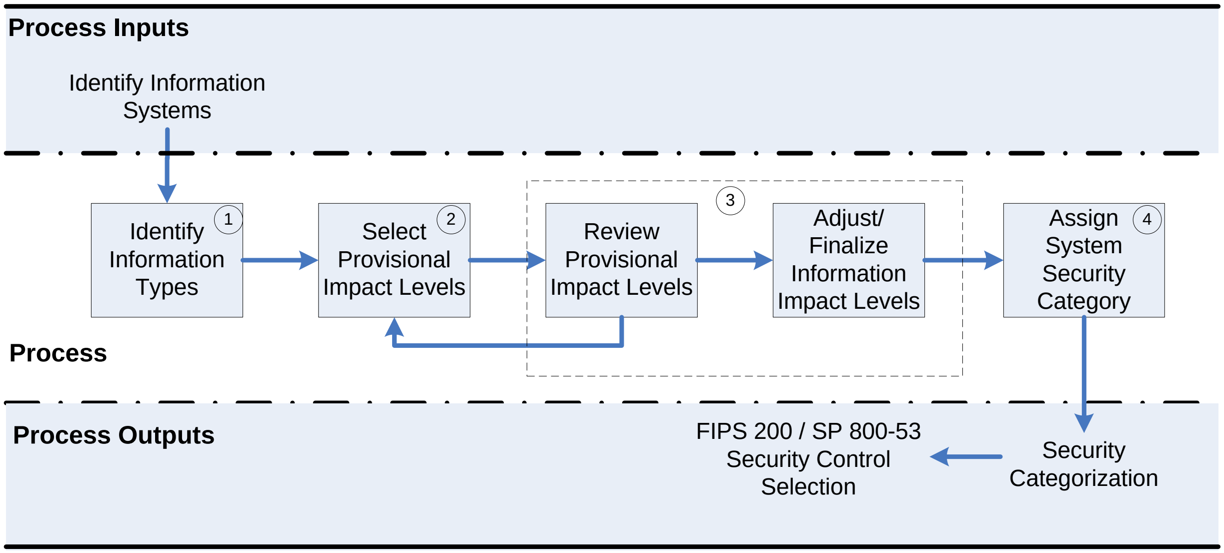

Process Inputs
Identify Information Systems
Identify Information Types
1
Select Provisional Impact Levels
2
3
Review Provisional Impact Levels
Adjust/ Finalize Information Impact Levels
Assign System Security Category
4
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

Figure 2: SP 800-60 Security Categorization Process Execution

Table 3 provides a step-by-step roadmap for identifying information types, establishing security impact levels for loss of confidentiality, integrity, and availability of information types, and assigning security categorization for the information types and for the information systems. Security categorization is the basis for identifying an initial baseline set of security controls for the information system.[10] Each functional step in the process is explained in detail in Sections 4.1 through 4.4.

[10] An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information [Source: SP 800-53; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3502; OMB Circular A-130, App. III]

Table 3: SP 800-60 Process Roadmap

Process Step	Activities	Roles
Input: Identify information systems	• Agencies should develop their own policies regarding information system identification for security categorization purposes. The system is generally bounded by a security perimeter[11].	CIO; SAISO; Mission Owners
Step 1 Identify Information Types	• Document the agency's business and mission areas • Identify all of the information types that are input, stored, processed, and/or output from each system [Section 4.1] o Identify *Mission–based* Information Type categories based on supporting FEA Lines of Business [Section 4.1.1] o As applicable, identify *Management and Support* Information Type categories based on supporting FEA Lines of Business [Section 4.1.2] o Specify applicable sub-functions for the identified *Mission-based* and *Management and Support* categories [Volume II, Appendices C and D] o As necessary, identify other required information types [Sections 4.1.3, 4.1.4] • Document applicable information types for the identified information system along with the basis for the information type selection [Section 4.5]	Mission Owners; Information Owners
Step 2 Select Provisional Impact Levels	• Select the security impact levels for the identified information types o from the recommended provisional impact levels for each identified information type [Volume II, Appendices C and D] o or, from FIPS 199 criteria provided in Table 7 Section 4.2.1, and Section 4.2.2 • Determine the security category (SC) for each information type: $SC_{\text{information type}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)} • Document the provisional impact level of confidentiality, integrity, and availability associated with the system's information type [Section 4.5]	Information System Security Officer (ISSO)
Step 3 Review Provisional Impact Levels Adjust/ Finalize Information Impact Levels	• Review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing [Section 4.3] • Adjust the impact levels as necessary based on the following considerations: o Confidentiality, integrity, and availability factors [Section 4.2.2] o Situational and operational drivers (timing, lifecycle, etc.) [Section 4.3] o Legal or statutory reasons • Document all adjustments to the impact levels and provide the rationale or justification for the adjustments [Section 4.5]	SAISO; ISSO; Mission Owners; Information Owners
Step 4 Assign System Security Category	• Review identified security categorizations for the aggregate of information types. • Determine the system security categorization by identifying the security impact level high water mark for each of the security objectives (confidentiality, integrity, availability): $SC_{\text{System X}}$ = {(confidentiality, impact), (integrity, impact), (availability, impact)} • Adjust the security impact level high water mark for each system security objective, as necessary, by applying the factors discussed in section 4.4.2. • Assign the overall information system impact level based on the highest impact level for the system security objectives (confidentiality, integrity, availability) • Follow the agency's oversight process for reviewing, approving, and documenting all determinations or decisions [Section 4.5]	CIO, SAISO; ISSO; Mission Owners; Information Owners
Output: Security Categorization	• Output that can be used as input to the selection of the set of security controls necessary for each system and the system risk assessment • The minimum security controls recommended for each system security category can be found in NIST SP 800-53, as updated	CIO; ISSO; Authorizing Officials; Developers

[11] Security perimeter is synonymous with the term accreditation boundary and includes all components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected.

4.1 Step 1: Identify Information Types

In accordance with FIPS 199, agencies shall identify all of the applicable information types that are representative of input, stored, processed, and/or output data from each system. The initial activity in mapping types of Federal information and information systems to security objectives and impact levels is the development of an information taxonomy, or creation of a catalog of information types.[12] The basis for the identification of information types is the OMB's Business Reference Model (BRM) described in the October 2007 publication, *FEA Consolidated Reference Model Document, Version 2.3*. The *BRM* describes four business areas containing 39 FEA lines of business.[13] The four business areas separate government operations into high-level categories relating:

- The purpose of government (*services for citizens*);
- The mechanisms the government uses to achieve its purpose (*mode of delivery*);
- The support functions necessary to conduct government operations (*support delivery of services*); and
- The resource management functions that support all areas of the government's business (*management of government resources*).

The first two business areas, *services for citizens* and the *mode of delivery* represent the NIST SP 800-60 Mission-based Information Types and will be discussed first in the following section, while *support delivery of services* and *management of government resources* represent Management and Support Information Types and will be presented in Section 4.1.2.

Although this guideline identifies a number of information types and bases its taxonomy on the *BRM*, only a few of the types identified are likely to be processed by any single system. Also, each system may process information that does not fall neatly into one of the listed information types. Once a set of information types identified in this guideline has been selected, it is prudent to review the information processed by each system under review to see if additional types need to be identified for impact assessment purposes. Also, it is recommended that organizational officials maintain proper documentation of identified information types per information system along with the basis for the information type selection. Guidance for documenting information types is provided in Section 4.5.

4.1.1 Identification of Mission-based Information Types

This section describes a process for identifying mission-based information types and for specifying the impact of unauthorized disclosure, modification, or unavailability of this information. Mission-based information types are, by definition, specific to individual departments and agencies or to specific sets of departments and agencies. The BRM *services for citizens* business area provides the primary frame of reference for determining the security

[12] One issue associated with the taxonomy activity is the determination of the degree of granularity. If the categories are too broad, then the guidelines for assigning impact levels are likely to be too general to be useful. On the other hand, if an attempt is made to provide guidelines for each element of information processed by each government agency, the guideline is likely to be unwieldy and to require excessively frequent changes.

[13] Definitions are provided in SP 800-60 Appendix A for the BRM terms such as "Business Areas", "Lines of Businesses" and "Sub-functions".

objectives impact levels for mission-based information and information systems. The consequences or impact of unauthorized disclosure of information, modification or destruction of information, and disruption of access to or use of information are defined by the nature and beneficiary of the service being provided or supported. The BRM establishes 26 direct services and delivery support lines of business with 98 associated information types (reference Table 4). Two additional information types were included to address Executive Functions of the Executive Office of the President and Trade Law Enforcement. These additions are identified by italics in Table 4.

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Mission Areas and Information Types [Services for Citizens]

D.1 Defense & National Security
Strategic National & Theater Defense
Operational Defense
Tactical Defense

D.2 Homeland Security
Border and Transportation Security
Key Asset and Critical Infrastructure Protection
Catastrophic Defense
Executive Functions of the Executive Office of the President (EOP)

D.3 Intelligence Operations
Intelligence Planning
Intelligence Collection
Intelligence Analysis & Production
Intelligence Dissemination
Intelligence Processing

D.4 Disaster Management
Disaster Monitoring and Prediction
Disaster Preparedness and Planning
Disaster Repair and Restoration
Emergency Response

D.5 International Affairs & Commerce
Foreign Affairs
International Development and Humanitarian Aid
Global Trade

D.6 Natural Resources
Water Resource Management
Conservation, Marine and Land Management
Recreational Resource Management and Tourism
Agricultural Innovation and Services

D.7 Energy
Energy Supply
Energy Conservation and Preparedness
Energy Resource Management
Energy Production

D.8 Environmental Management
Environmental Monitoring and Forecasting
Environmental Remediation
Pollution Prevention and Control

D.9 Economic Development
Business and Industry Development
Intellectual Property Protection
Financial Sector Oversight
Industry Sector Income Stabilization

D.10 Community & Social Services
Homeownership Promotion
Community and Regional Development
Social Services
Postal Services

D.11 Transportation
Ground Transportation
Water Transportation
Air Transportation
Space Operations

D.12 Education
Elementary, Secondary, and Vocational Education
Higher Education
Cultural and Historic Preservation
Cultural and Historic Exhibition

D.13 Workforce Management
Training and Employment
Labor Rights Management
Worker Safety

D.14 Health
Access to Care
Population Health Mgmt & Consumer Safety
Health Care Administration
Health Care Delivery Services
Health Care Research and Practitioner Education

D.15 Income Security
General Retirement and Disability
Unemployment Compensation
Housing Assistance
Food and Nutrition Assistance
Survivor Compensation

D.16 Law Enforcement
Criminal Apprehension
Criminal Investigation and Surveillance
Citizen Protection
Leadership Protection
Property Protection
Substance Control
Crime Prevention
Trade Law Enforcement

D.17 Litigation & Judicial Activities
Judicial Hearings
Legal Defense
Legal Investigation
Legal Prosecution and Litigation
Resolution Facilitation

D.18 Federal Correctional Activities
Criminal Incarceration
Criminal Rehabilitation

D.19 General Sciences & Innovation
Scientific and Technological Research and Innovation
Space Exploration and Innovation

[14] The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, October 2007.

Table 4: Mission-Based Information Types and Delivery Mechanisms[14]

Services Delivery Mechanisms and Information Types [Mode of Delivery]

D.20 Knowledge Creation & Management

Research and Development
General Purpose Data and Statistics
Advising and Consulting
Knowledge Dissemination

D.21 Regulatory Compliance & Enforcement

Inspections and Auditing
Standards Setting/Reporting Guideline Development
Permits and Licensing

D.22 Public Goods Creation & Management

Manufacturing
Construction
Public Resources, Facility and Infrastructure Management
Information Infrastructure Management

D.23 Federal Financial Assistance

Federal Grants (Non-State)
Direct Transfers to Individuals
Subsidies
Tax Credits

D.24 Credit and Insurance

Direct Loans
Loan Guarantees
General Insurance

D.25 Transfers to State/ Local Governments

Formula Grants
Project/Competitive Grants
Earmarked Grants
State Loans

D.26 Direct Services for Citizens

Military Operations
Civilian Operations

The approach to establishing mission-based information types at an agency level begins by documenting the agency's business and mission areas. The owner, or designee, of each information system is responsible for identifying the information types stored in, processed by, or generated by that information system. In the case of mission-based information, the responsible individuals, in coordination with management, operational, and security stakeholders, should compile a comprehensive set of lines of business and mission areas conducted by the agency. In addition, the responsible individuals should identify the applicable sub-functions necessary to conduct agency business and in turn accomplish the agency's mission. For example, one mission conducted by an agency might be law enforcement. Sub-functions that are part of the agency's law enforcement mission might include criminal investigation and surveillance, criminal apprehension, criminal incarceration, citizen protection, crime prevention, and property protection. Each of these sub-functions would represent an information type.

Recommended mission-based lines of business and constituent sub-functions that may be processed by information systems are identified in Table 4 with details provided in Volume II, Appendix D, "Examples of Impact Determination for Mission-based Information and Information Systems."

Implementation Tip

At the agency level, all government agencies perform at least one of the *mission areas* and employ at least one of the *services delivery mechanisms* described in Table 4. However, some information systems may only provide a supporting role to the agency's mission and not directly process any of the *mission-based* information types.

4.1.2 Identification of Management and Support Information

Much Federal government information and many supporting information systems are not employed directly to provide direct mission-based services, but are primarily intended to support delivery of services or to manage resources. The *support delivery of services* and *management of resources* business areas are together composed of 13 lines of business (Tables 5 and 6). The

BRM subdivides the lines of business into 72 sub-functions. The *support delivery of services* and *management of resource* business areas are common to most Federal government agencies, and the information associated with each of their sub-functions is identified in this guideline as a *management and support* information type. Four additional *management and support* sub-factor information types have been defined to address privacy information. One additional *management and support* sub-factor information type has been defined to address General Information as a catch-all information type that may not be defined by the FEA BRM. As such, agencies may find it necessary to identify additional information types not defined in the BRM and assign associated security impact levels to those types.

4.1.2.1 Services Delivery Support Information

Most information systems employed in both service delivery support and resource management activities engage in one or more of the eight *support delivery of services* lines of business. Each of the information types associated with *support delivery of services* sub-functions is provided in Table 5. Volume II, Appendix C.2, "Services Delivery Support Functions," recommends provisional impact levels for confidentiality, integrity, and availability security objectives. These service support functions are the day-to-day activities necessary to provide the critical policy, programmatic, and managerial foundation that support Federal government operations. The direct service missions and constituencies ultimately being supported by service support functions comprise a significant factor in determining the security impacts associated with compromise of information associated with the *support delivery of services* business area.

Table 5: Services Delivery Support Functions and Information Types[15]

C.2.1 Controls and Oversight	**C.2.4 Internal Risk Management & Mitigation**	**C.2.8 General Government**
Corrective Action (Policy/Regulation)		Central Fiscal Operations
Program Evaluation	Contingency Planning	Legislative Functions
Program Monitoring	Continuity of Operations	Executive Functions
C.2.2 Regulatory Development	Service Recovery	Central Property Management
Policy & Guidance Development	**C.2.5 Revenue Collection**	Central Personnel Management
Public Comment Tracking	Debt Collection	Taxation Management
Regulatory Creation	User Fee Collection	Central Records & Statistics Management
Rule Publication	Federal Asset Sales	
C.2.3 Planning & Budgeting	**C.2.6 Public Affairs**	*Income Information*
Budget Formulation	Customer Services	*Personal Identity and Authentication*
Capital Planning	Official Information Dissemination	*Entitlement Event Information*
Enterprise Architecture	Product Outreach	*Representative Payee Information*
Strategic Planning	Public Relations	*General Information*
Budget Execution	**C.2.7 Legislative Relations**	
Workforce Planning	Legislation Tracking	
Management Improvement	Legislation Testimony	
Budgeting & Performance Integration	Proposal Development	
Tax & Fiscal Policy	Congressional Liaison Operations	

4.1.2.2 Government Resource Management Information

The *government resource management information* business area includes the back office support activities enabling the Federal government to operate effectively. The five *government resource management information* lines of business and the sub-functions associated with each

[15] The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, October 2007.

information type are identified in Table 6. Volume II, Appendix C.3, "Government Resource Management Information," recommends provisional impact levels for confidentiality, integrity, and availability security objectives. Many departments and agencies operate their own support systems. Others obtain at least some support services from other organizations. Some agencies' missions are primarily to support other government departments and agencies in the conduct of direct service missions. As indicated above, security objectives and associated security impact levels for administrative and management information and systems are determined by the nature of the supported direct services and constituencies being supported.

Table 6: Government Resource Management Functions and Information Types[16]

C.3.1 Administrative Management	**C.3.3 Human Resource Management**	**C.3.5 Information & Technology Management**
Facilities, Fleet, and Equipment Management	HR Strategy	
	Staff Acquisition	System Development
Help Desk Services	Organization & Position Mgmt	Lifecycle/Change Management
Security Management	Compensation Management	System Maintenance
Travel	Benefits Management	IT Infrastructure Maintenance
Workplace Policy Development & Management	Employee Performance Mgmt	Information Security
	Employee Relations	Record Retention
C.3.2 Financial Management	Labor Relations	Information Management
Accounting	Separation Management	System and Network Monitoring
Funds Control	Human Resources Development	Information Sharing
Payments	**C.3.4 Supply Chain Management**	
Collections and Receivables	Goods Acquisition	
Asset and Liability Management	Inventory Control	
Reporting and Information	Logistics Management	
Cost Accounting/ Performance Measurement	Services Acquisition	

4.1.3 Legislative and Executive Information Mandates

During the identification of information types within an information system, agency personnel should afford special consideration for applicable governances addressing the information processed and the agency's supported mission. Volume II, Appendix E lists legislative and executive mandates establishing sensitivity and criticality guidelines for specific information types.

4.1.4 Identifying Information Types Not Listed in this Guideline

The FEA BRM Information Types are provided only as a taxonomy guideline. Not all information processed by an information system may be identified from Tables 4 through 6. Therefore, an agency may identify unique information types not listed in this guideline or may choose not to select provisional impact levels from Volume II, Appendix C (for management and support information types) or Volume II, Appendix D (for mission-based information types). Sections 4.2.1 through 4.2.3 of this guideline provide assistance to agencies in assigning provisional security categories to agency-identified information types and information systems.

Additionally, SP 800-60 provides a *management and support* sub function, General Information Type, which can be used by agencies as a means to identify and categorize information not

[16] The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3, October 2007.

contained in the FEA BRM. A complete description of the General Information Type information should be captured in the agency's collection and documentation process.

4.2 Step 2: Select Provisional Impact Level

In Step 2, organizations should establish provisional impact levels[17] based on the identified information types in Step 1. The provisional impact levels are the original impact levels assigned to the confidentiality, integrity, and availability security objectives of an information type from Volume II before any adjustments are made. Also in this step, the initial security categorization for the information type is established and documented.

Volume II, Appendix C suggests provisional confidentiality, integrity, and availability impact levels for management and support information types, and Volume II, Appendix D provides examples of provisional impact level assignments for mission-based information types. Using the impact assessment criteria identified in Section 3.2 for the security objectives and types of potential losses identified in Section 3.1.2, the organizational entity responsible for impact determination must assign impact levels and consequent security categorization for the *mission-based* and *management and support* information types identified for each information system.

4.2.1 FIPS 199 Security Categorization Criteria

Where an information type processed by an information system is not categorized by this guideline [based on information types identified in Volume II, Appendices C and D], an initial impact determination will need to be made based on FIPS 199 categorization criteria (cited in Table 7).

Agencies can assign security categories to information types and information systems by selecting and adjusting appropriate Table 7 values for the potential impact of compromises of confidentiality, integrity, and availability security objectives. Those responsible for impact level selection and subsequent security categorization should apply the criteria provided in Table 7 to each information type received by, processed in, stored in, and/or generated by each system for which they are responsible. The security categorization will generally be determined based on the most sensitive or critical information received by, processed in, stored in, and/or generated by the system under review.

[17] Impact levels (plural), as used here, refers to *low*, *moderate*, *high*, or *not applicable* values assigned to each security objective (i.e., confidentiality, integrity, and availability) used in expressing the security category of an information type or information systems. The value of *not applicable* only applies to information types and not to information systems.

Table 7: Categorization of Federal Information and Information Systems

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

4.2.2 Common Factors for Selection of Impact Levels

Where an agency determines security impact levels and security categorization based on local application of FIPS 199 criteria, it is recommended that the following factors be considered with respect to security impacts for each information type.

4.2.2.1 Confidentiality Factors

Using the FIPS 199 potential impact criteria summarized in Table 7, each information type should be evaluated for confidentiality with respect to the impact level associated with unauthorized disclosure of (i) each known variant of the information belonging to the type and (ii) each use of the information by the system under review. Answers to the following questions will help in the evaluation process:

- How can a malicious adversary use the unauthorized disclosure of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- How can a malicious adversary use the unauthorized disclosure of information to gain control of agency assets that might result in unauthorized modification of information, destruction of information, or denial of system services that would result in limited/serious/severe harm to agency operations, agency assets, or individuals?

- Would unauthorized disclosure/dissemination of elements of the information type violate laws, executive orders, or agency regulations?

4.2.2.2 Integrity Factors

Using the FIPS 199 potential impact criteria summarized in Table 7, each information type should be evaluated for integrity with respect to the impact level associated with unauthorized modification or destruction of (i) each known variant of the information belonging to the type and (ii) each use of the information by the system under review. Answers to the following questions will help in the evaluation process:

- How can a malicious adversary use the unauthorized modification or destruction of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- Would unauthorized modification/destruction of elements of the information type violate laws, executive orders, or agency regulations?

Unauthorized modification or destruction of information can take many forms. The changes can be subtle and hard to detect, or they can occur on a massive scale. One can construct an extraordinarily wide range of scenarios for modification of information and its likely consequences. Just a few examples include forging or modifying information to:

- Reduce public confidence in an agency;
- Fraudulently achieve financial gain;
- Create confusion or controversy by promulgating a fraudulent or incorrect procedure;
- Initiate confusion or controversy through false attribution of a fraudulent or false policy;
- Influence personnel decisions;
- Interfere with or manipulate law enforcement or legal processes;
- Influence legislation; or
- Achieve unauthorized access to government information or facilities.

In most cases, the most serious impacts of integrity compromise occur when some action is taken that is based on the modified information or the modified information is disseminated to other organizations or the public.

Undetected loss of integrity can be catastrophic for many information types. The consequences of integrity compromise can be either direct (e.g., modification of a financial entry, medical alert, or criminal record) or indirect (e.g., facilitation of unauthorized access to sensitive or private information or deny access to information or information system services). Malicious use of write access to information and information systems can do enormous harm to an agency's mission and can be employed to use an agency system as a proxy for attacks on other systems.

In many cases, the consequences of unauthorized modification or destruction of information to agency mission functions and public confidence in the agency can be expected to be limited. In other cases, integrity compromises can result in the endangerment of human life or other severe consequences. The impact can be particularly severe in the case of time-critical information.

4.2.2.3 Availability Factors

Using the FIPS 199 potential impact criteria summarized in Table 7, each information type should be evaluated for availability with respect to the impact level associated with the disruption of access to or use of information of (i) each known variant of the information belonging to the type and (ii) each use of the information by the system under review. Answers to the following questions will help in the evaluation process:

- How can a malicious adversary use the disruption of access to or use of information to do limited/serious/severe harm to agency operations, agency assets, or individuals?
- Would disruption of access to or use of elements of the information type violate laws, executive orders, or agency regulations?

For many information types and information systems, the availability impact level depends on how long the information or system remains unavailable. Undetected loss of availability can be catastrophic for many information types. For example, permanent loss of budget execution, contingency planning, continuity of operations, service recovery, debt collection, taxation management, personnel management, payroll management, security management, inventory control, logistics management, or accounting information databases would be catastrophic for almost any agency. Complete reconstruction of such databases would be time consuming and expensive.

In most cases, the adverse effects of a limited-duration availability compromise on an organization's mission functions and public confidence will be limited. In contrast, for time-critical information types, availability is less likely to be restored before serious harm is done to agency assets, operations, or personnel (or to public welfare). In such instances, the documented availability impact level recommendations should indicate the information is time-critical and the basis for criticality.

4.2.3 Examples of FIPS 199-Based Selection of Impact Levels

FIPS 199-based examples of security objective impact selection and security categorization for sample information types follow:

EXAMPLE 1: An organization managing *public information* on its web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability. The resulting security category of this information type is expressed as:

> Security Category $_{\text{public information}}$ = {(confidentiality, n/a), (integrity, moderate), (availability, moderate)}.

EXAMPLE 2: A law enforcement organization managing extremely sensitive *investigative information* determines that the potential impact from a loss of confidentiality is high, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is moderate. The resulting security category for this type of information is expressed as:

Security Category $_{\text{investigative information}}$ = {(confidentiality, high), (integrity, moderate), (availability, moderate)}.

EXAMPLE 3: A financial organization managing routine *administrative information* (not privacy-related information) determines that the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security category of this information type is expressed as:

Security Category $_{\text{administrative information}}$ = {(confidentiality, low), (integrity, low), (availability, low)}.

In general, security objective impact assessment is independent of mechanisms employed to mitigate the consequences of a compromise.

4.3 Step 3: Review Provisional Impact Levels and Adjust/Finalize Information Type Impact Levels

In Step 3, organizations should review and adjust the provisional security impact levels for the security objectives of each information type and arrive at a finalized state. To accomplish this, organizations should: (i) review the appropriateness of the provisional impact levels based on the organization, environment, mission, use, and data sharing; (ii) adjust the security objective impact levels as necessary using the special factors[18] guidance found in Volume II, Appendices C and D; and (iii) document all adjustments to the impact levels and provide the rationale or justification for the adjustments.

When security categorization impact levels recommended in Section 4.2 or Volume II, Appendices C and D are adopted as provisional security impact levels, the agency should review the appropriateness of the provisional impact levels in the context of the organization, environment, mission, use, and data sharing associated with the information system under review. This review should include the agency's mission importance; lifecycle and timeliness implications; configuration and security policy related information; special handling requirements; etc. The FIPS 199 factors presented in Section 4.2.2 of this document should be used as the basis for decisions regarding adjustment or finalization of the provisional impact levels. The confidentiality, integrity, and availability impact levels may be adjusted one or more times in the course of the review. Once the review and adjustment process is complete, the mapping of impact levels by information type can be finalized.

The impact of information compromise of a particular type can vary in different agencies or in dissimilar operational contexts. Also, the impact for an information type may vary throughout the life cycle. For example, contract information that has a ***moderate*** confidentiality impact level during the life of the contract may have a ***low*** impact level when the contract is completed. Policy information may have ***moderate*** confidentiality and integrity impact levels during the policy development process, ***low*** confidentiality and ***moderate*** integrity impact levels when the policy is implemented, and ***low*** confidentiality and integrity impact levels when the policy is no longer used.

[18] The special factor guidance in NIST SP 800-60, Volume II, provides specific guidance on considerations for adjusting each security objective (confidentiality, integrity, and availability) for each information type. The special factor guidance is applied to each information type, based on how the information type is used, the organization's mission, or the system's operating environment.

The impact levels associated with the *management and support* information common to many agencies are strongly affected by the *mission-based* information with which it is associated. That is, agency-common management and support information used with very sensitive or critical mission-based information types may have higher impact levels than the same agency-common information used with less critical mission-based information types.

Further, information systems process many types of information. Not all of these information types are likely to have the same security impact levels. The compromise of some information types will jeopardize system functionality and agency mission more than the compromise of other information types. System security impact levels must be assessed in the context of system mission and function as well as on the basis of the aggregate of the component information types.

Additionally, configuration and security policy enforcement information should be reviewed and adjusted considering the information processed on the system. Configuration and security policy information includes password files, network access rules, other hardware and software configuration settings, and documentation affecting access to the information system's data, programs, and/or processes. At a minimum, a low confidentiality and integrity impact level will apply to this set of information and processes due to a potential for corruption, misuse, or abuse of system information and processes.

A factor specific to the confidentiality objective is information subject to special handling (e.g., information subject to the Privacy Act of 1974, 5 U.S.C. § 552A). Regardless of other considerations, some minimum confidentiality impact level must be assigned to any information system that stores, processes, or generates such information. Examples of such information include information subject to the Trade Secrets Act, the Privacy Act, Department of Energy Safeguards Information, Internal Revenue Service Official Use Only Information, and Environmental Protection Agency Confidential Business Information (e.g., subject to Toxic Substances Control Act; Resource Conservation and Recovery Act; Comprehensive Environmental Response, Compensation, and Liability Act). Some of these statutory and regulatory specifications are listed in Volume II, Appendix E, "Legislative and Executive Sources Establishing Sensitivity/Criticality."

4.4 Step 4: Assign System Security Category

Once the security impact levels have been selected, reviewed and adjusted as necessary for the security objectives of each individual information type processed by an information system, it is necessary to assign a system security category based on the aggregate of information types. The Step 4 activities include the following: (i) review identified security categorizations for the aggregate of information types; (ii) determine the system security categorization by identifying the high water mark for each of the security objectives (confidentiality, integrity, availability) based on the aggregate of the information types; (iii) adjust the high water mark for each system security objective, as necessary, by applying the factors discussed in section 4.4.2; (iv) assign the overall information system impact level based on the highest impact level for the system security objectives; and (v) document all security categorization determinations and decisions.

4.4.1 FIPS 199 Process for System Security Categorization

FIPS 199 recognizes that determining the security category of an information system requires additional analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential security impact levels assigned to each of the respective security objectives (confidentiality, integrity, availability) are the highest level (i.e., high water mark) for any one of these objectives that has been determined for the types of information resident on the information system.

Information systems are composed of both computer programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential business functions and operations. These system-processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate worst case potential for the overall information system—thereby obviating the need to consider the system processes in the security categorization of the information system. This is in recognition of:

- The fundamental requirement to protect the integrity, availability, and, for key information such as passwords and encryption keys, the confidentiality of system-level processing functions and information at the high water mark; and
- The strong interdependence between confidentiality, integrity, and availability.

For this reason, FIPS 199 notes that, while the value (i.e., level) of *not applicable* can apply to a security objective for specific information types processed by systems, this value cannot be assigned to any security objective for an information system. There is a minimum provisional impact (i.e., low water mark) for a compromise of confidentiality, integrity, and availability for an information system. This is necessary to protect the system-level processing functions and information critical to the operation of the information system.

The generalized format for expressing the security category, or *SC*, of an information system is:

$$SC_{\text{information system}} = \{(\text{confidentiality}, \textit{impact}), (\text{integrity}, \textit{impact}), (\text{availability}, \textit{impact})\},$$

where the acceptable values for potential impact are LOW, MODERATE, or HIGH.

The following examples illustrate the system security categorization process described in FIPS 199.

SYSTEM EXAMPLE 1: An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. The management within the contracting organization determines that: (i) for the sensitive contract information, the potential impact from a loss of confidentiality is moderate, the potential impact from a loss of integrity is moderate, and the potential impact from a loss of availability is low; and (ii) for the routine administrative information (non-privacy-related information), the potential impact from a loss of confidentiality is low, the potential impact from a loss of integrity is low, and the potential impact from a loss of availability is low. The resulting security categories, or *SC*, of these information types are expressed as:

SC $_{\text{contract information}}$ = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)}, and

SC $_{\text{administrative information}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting security category of the information system is expressed as:

SC $_{\text{acquisition system}}$ = {(confidentiality, MODERATE), (integrity, MODERATE), (availability, LOW)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the acquisition system.

SYSTEM EXAMPLE 2: A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution f electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. The management at the power plant determines that: (i) for the sensor data being acquired by the SCADA system, there is no potential impact from a loss of confidentiality, a high potential impact from a loss of integrity, and a high potential impact from a loss of availability; and (ii) for the administrative information being processed by the system, there is a low potential impact from a loss of confidentiality, a low potential impact from a loss of integrity, and a low potential impact from a loss of availability. The resulting security categories, or *SC*, of these information types are expressed as:

SC $_{\text{sensor data}}$ = {(confidentiality, NA), (integrity, HIGH), (availability, HIGH)}, and

SC $_{\text{administrative information}}$ = {(confidentiality, LOW), (integrity, LOW), (availability, LOW)}.

The resulting security category of the information system is initially expressed as:

SC $_{\text{SCADA system}}$ = {(confidentiality, LOW), (integrity, HIGH), (availability, HIGH)},

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the SCADA system. The management at the power plant chooses to increase the potential impact from a loss of confidentiality from low to moderate reflecting a more realistic view of the potential impact on the information system should there be a security breach due to the unauthorized disclosure of system-level information or processing functions. The final security category of the information system is expressed as:

SC $_{\text{SCADA system}}$ = {(confidentiality, MODERATE), (integrity, HIGH), (availability, HIGH)}.

4.4.2 Guidelines for System Categorization

In some cases, the impact level for a system security category will be higher than any security objective impact level for any information type processed by the system.

The primary factors that most commonly raise the impact levels of the system security category above that of its constituent information types are aggregation and critical system functionality. Additionally, variations in sensitivity/criticality with respect to time may need to be factored into the impact assignment process. Some information loses its sensitivity in time (e.g., economic/commodity projections after they've been published). Other information is particularly critical at some point in time (e.g., weather data in the terminal approach area during aircraft landing operations). This section provides some general guidelines regarding how aggregation, critical functionality, and other system factors may affect system security categorization.

Implementation Tip

Agency personnel should be aware that there are several factors that should be considered during the aggregation of system information types. When considering these factors, previously unforeseen concerns may surface affecting the confidentiality, integrity, and/or availability impact levels at the system level. These factors include data aggregation, critical system functionality, extenuating circumstances, and other system factors.

In order to effectively accomplish this step, various stakeholders (e.g., management, operational personnel, or security experts) may need to be involved in decisions regarding system-level impact assessments. The following sections provide factors to consider in adjusting the system security objective impact levels.

4.4.2.1 Aggregation

Some information may have little or no sensitivity in isolation but may be highly sensitive in aggregation. In some cases, aggregation of large quantities of a single information type can reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems. In other cases, aggregation of information of several different and seemingly innocuous types can have similar effects. In general, the sensitivity of a given data element is likely to be greater in context than in isolation (e.g., association of an account number with the identity of an individual and/or institution). The availability, routine operational employment, and sophistication of data aggregation and inference tools are all increasing rapidly. If review reveals increased sensitivity or criticality associated with information aggregates, then the system security objective impact levels may need to be adjusted to a higher level than would be indicated by the security impact levels associated with any individual information type. This could be implemented by incorporating a statement that explains the aggregation and potential security objective affected as well as the modification to impact levels.

4.4.2.2 Critical System Functionality

Compromise of some information types may have low impact in the context of a system’s primary function but may have much more significance when viewed in the context of the potential impact of compromising:

- Other systems to which the system in question is connected, or
- Other systems which are dependent on that system’s information.

Access control information for a system that processes only low impact information might initially be thought to have only low impact security objectives. However, if access to that system might result in some form of access to other systems (e.g., over a network), the sensitivity and criticality attributes of all systems to which such indirect access can result needs to be considered. Similarly, some information may, in general, have low sensitivity and/or criticality security objectives. However, that information may be used by other systems to enable extremely sensitive or critical functions (e.g., air traffic control use of weather information or use of commercial flight information to identify military combat transport systems). Loss of data integrity, availability, temporal context, or other context can have catastrophic consequences.

4.4.2.3 Extenuating Circumstances

This publication focuses on categorizing an information system based on its information types and associated security objective impacts. There are times when a system security objective impact level should be elevated based on reasons other than its information. For example, the information system provides critical process flow or security capability, the visibility of the system to the public, the sheer number of other systems reliant on its operation or possibly its overall cost of replacement. These examples, given a specific situation, may provide reason for the system owner to increase the overall security impact level of a system.

An elevation based on extenuating circumstances can be more apparent by comparing the original security categorization to the business impact analysis. If the system was categorized based on FIPS 199 at a Moderate overall impact level but the system owner has determined it needs to be operational within 4-8 hours of a disruption irrespective of the aggregated information type availability security impact level assigned, then there is a disconnect that might be caused by the system's extenuating circumstances. Agencies must customize the information system availability security impact level as appropriate to obtain full value and accuracy.

4.4.2.4 Other System Factors

Public Information Integrity

Most Federal agencies maintain web pages that are accessible to the public. The vast majority of these public web pages permit interaction between the site and the public. In some cases, the site provides only information. In other cases, forms may be submitted via the website (e.g., applications for service or job applications). In some cases, the site is a medium for business transactions. Unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) may adversely affect operations and/or public confidence in the agency. In most cases, the damage can be corrected within a relatively short period of time, and the damage is limited (impact level is ***low***). In other cases (e.g., very large fraudulent transactions or modification of a web page belonging to an intelligence/security community component), the damage to mission function and/or public confidence in the agency can be serious. In such cases, the integrity impact associated with unauthorized modification or destruction of a public web page would be at least ***moderate***.

Catastrophic Loss of System Availability

Either physical or logical destruction of major assets can result in very large expenditures to restore the assets and/or long periods of time for recovery. Permanent loss/unavailability of information system capabilities can seriously hamper agency operations and, where direct services to the public are involved, have a severe adverse effect on public confidence in Federal agencies. Particularly in the case of large systems, FIPS 199 criteria suggest that catastrophic loss of system availability may result in a ***high*** availability impact level. Whether or not the impact level of system availability should be ***high*** (and subsequent ***high*** system security impact level) is dependent on other factors, such as cost and criticality of the system, rather than on the security impact levels for the information types being processed by the system.

Large Supporting and Interconnecting Systems

Large or complex information systems composed of multiple lower level systems often require additional consideration regarding assignment of system security categorization. This section will provide guidelines for applying and interrelating individual system security categorization results to enterprise organizations, large supporting infrastructures (such as general support systems, data warehouse applications, large data storage units, server farms, and information repositories), and interconnecting systems.

Upon security categorization identification for all information systems interacting with large infrastructure systems, senior IT and security officials have possession of valuable information that can now enable an enterprise wide security perspective. One significant activity includes levying an overall security categorization for the agency's supporting network infrastructures. Since networks, as well as other general support systems, do not inherently "own" mission-based or management and support information types, the infrastructure's categorization is based on the aggregation of the information systems' security categorizations. In other words, the infrastructure's security categorization is the high water mark of the supported information systems and is based on the information types processed, flowed, or stored on the network or general support system. Together, the top down enterprise wide threat assessment and bottom up security assessment derived by aggregation will allow an organization to look at its risk profile from a comprehensive and balanced view. Further, this analysis will ensure the proper application of common security controls supporting the multiple information systems and the protection provided by those controls are inherited by the individual systems.

Critical Infrastructures and Key Resources

Where the mission served by an information system, or the information that the system processes, affects the security of critical infrastructures and key resources, the harm that results from a compromise requires particularly close attention. In this case, an effect on security might include a significant reduction in the effectiveness of physical or cyber security protection mechanisms, or facilitation of a terrorist attack on critical infrastructures and key resources. Accordingly, the system security categorization should be carefully determined when a loss of confidentiality, integrity, or availability will result in a negative impact on the critical infrastructures and key resources.

The *Critical Information Infrastructure Act of 2002*, Public Law 107-296 §§ 211-215 of November 25, 2002 (codified as 6 U.S.C. 131-134), defines the term "critical infrastructure information" to mean information not customarily in the public domain and related to the security of critical infrastructure or protected systems. Should information types be aligned with Critical Infrastructures, then action should be taken to ensure compliance with Homeland Security Presidential Directive No. 7 (HSPD 7) and to initiate an interdependency analysis.

Privacy Information

The E-Government Act of 2002 complements privacy protection requirements of the *Privacy Act of 1974*. Under the terms of these public laws, Federal government agencies have specific responsibilities regarding collection, dissemination or disclosure of information regarding individuals.[19]

The September 26, 2003 OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," puts the privacy provisions of the E-Government Act of 2002 into effect. The guidance applies to information that identifies individuals in a recognizable form, including name, address, telephone number, Social Security Number, and e-mail addresses. OMB instructed agency heads "to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected." Under these public laws and executive policies, it is necessary to broaden the definition of "unauthorized disclosure" to encompass *any* access, use, disclosure, or sharing of privacy-protected information among Federal government agencies when such actions are prohibited by privacy laws and policies. Since most privacy regulations focus on access, use, disclosure, or sharing of information, privacy considerations are dealt with in this guideline as special factors affecting the confidentiality impact level. In establishing confidentiality impact levels for each information type, responsible parties must consider the consequences of unauthorized disclosure of privacy information (with respect to violations of Federal policy and/or law).

Agencies are required to conduct Privacy Impact Assessments (PIAs) before developing IT systems that contain personally identifiable information or before collecting personally identifiable information electronically. The impact of privacy violations should consider any adverse effects experienced by individuals or organizations as a result of the loss of PII confidentiality. Examples of adverse effects experienced by individuals may include blackmail, identity theft, discrimination, or emotional distress. Examples of adverse effects experienced by organizations may include administrative burden, financial losses, loss of public reputation and confidence, and the penalties associated with violation of the relevant statutes and policies.

Categorizations should be reviewed to ensure that the adverse effects of a loss of PII confidentiality have been adequately factored into impact determinations. The confidentiality impact level should generally fall into the ***moderate*** range.

Trade Secrets

There are several laws that specifically prohibit unauthorized disclosure of trade secrets (e.g., 7 U.S.C., Chapter 6, Subchapter II, Section 136h and 42 U.S.C., Chapter 6A, Subchapter XII, Part E, Section 300j-4(d)(1)). Systems that store, communicate, or process trade secrets will generally be assigned at least a ***moderate*** confidentiality impact level.

4.4.3 Overall Information System Impact

Since the impact values (i.e., levels) for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept[20] is used to

[19] The OMB definition of an individual is, "a citizen of the United States or an alien lawfully admitted for permanent residence." Agencies may choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

determine the overall impact level of the information system. The security impact level for an information system will generally be the highest impact level for the security objectives (confidentiality, integrity, and availability) associated with the aggregate of system information types. Thus, a low-impact system is defined as an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high.

4.5 Documenting the Security Categorization Process

Essential to the security categorization process is documenting the research, key decisions and approvals, and supporting rationale driving the information system security categorization. This information is key to supporting the security life cycle and will need to be included in the information system's security plan.

Figure 3 provides an example of information details that should be collected.

[20] The high water mark concept is employed because there are significant dependencies among the security objectives of confidentiality, integrity, and availability. In most cases, a compromise in one security objective ultimately affects the other security objectives as well.

Information System Name: SCADA System [and Agency specific identifier]			
Business and Mission Supported: The SCADA (supervisory control and data acquisition) system provides real-time control and information supporting the main power plant. The power plant provides critical distribution of electric power to the military installation.			
Information Types			
[D.7.1] Energy Supply	Sensor data monitoring the availability of energy for the Military installation and its soldiers and command authority. This function includes control of distribution and transfer of power. The SCADA remote control capabilities can take action such as initiating necessary switching actions to alleviate an overloading power condition. The impacts to this information and the SCADA system may affect the installation's critical infrastructures.		
[C.2.8.12]General Information	The SCADA information system processes routine administrative information.		
Step 1 **Identify Information Types**	**Step 2 [Provisional] / Step 3a [Adjustments]**		
	Confidentiality Impact	**Integrity Impact**	**Availability Impact**
	Step 3b- Impact Adjustment Justification		
Energy Supply	L / M	L / H	L / H
	Disclosure of sensor information may seriously impact the missions if indications & warnings of overall capability are provided to an adversary.	Severe impacts or consequences may occur if adversarial modification of information results in incorrect power system regulation or control actions.	Due to loss of availability, severe impact to the mission capability may result and may in-turn have overall catastrophic consequences for the facility's critical infrastructures and possible loss of human life.
General Information	L	L	L
	No adjustments	No adjustments	No adjustments
Step 4 System Categorization:	**Moderate**	**High**	**High**
	Overall Information System Impact: High		

Figure 3: Security Categorization Information Collection

In addition, agencies may consider enhancing their SSPs with other analyses, decisions, assignments, and or approvals that were used in the categorization process. Examples may include:

- Agency's business and mission areas (Step 1 in Table 1)
- Legislative and executive information mandates affecting the information impact assignment or adjustment (Section 4.1.3)
- Indicating whether the information is time-critical in rationales for assigning availability impact levels (Section 4.2.2.3)
- Rationales for assigning information to the General Information Type (Section 4.1.2, Implementation Tip)
- Results of reviews of the appropriateness of the provisional impact levels for information (Section 4.3)

- Results of considering the potential impacts to other organizations and considering, "in accordance with the USA Patriot Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system" (NIST SP 800-53 security control RA-2)
- Results of reviewing the identified security categorizations for the aggregate of information types (Step 4 in Table 1)
- Effects of various factors and circumstances (e.g., data aggregation, critical system functionality, privacy, trade secrets, critical infrastructure, aggregation, critical system functionality, extenuating circumstances) on the system category (Section 4.4.2)
- Whether and why the agency determined that the system impact level must be higher than any of the levels of the information types that the system processes (Section 4.4)
- Approvals of all determinations or decisions (Step 4 in Table 1)

4.6 Uses of Categorization Information

The results of system security categorization can and should be used by, or made available to, appropriate agency personnel to support agency activities including:

- Business Impact Analysis (BIA): Agency personnel should consider the cross-utilization of security categorization and BIA information in the performance of each activity. Their common objectives enable agencies to mutually draw from them, thus, providing checks and balances to ensure accuracy for each information system. Conflicting information and anomalous conditions, such as a low availability impact and a BIA three-hour recovery time objective, should trigger a reevaluation by the mission and data owners.
- Capital Planning and Investment Control (CPIC) and Enterprise Architecture (EA): Just as no IT investment should be made without a business-approved architecture,[21] the security categorization that begins the security life cycle is a business-enabling activity directly feeding the enterprise architecture and CPIC processes for new investments, as well as migration and upgrade decisions. Specifically, the security categorization can provide a firm basis for justifying certain capital expenditures and also can provide analytical input to avoid unnecessary investments.
- System Design: Understanding and designing the system architecture with varying information sensitivity levels in mind may assist in achieving economies of scale with security services and protection through common security zones within the enterprise. For example, an information system containing privacy information may be located in one security zone with other information systems containing similar sensitive information. Each zone may have varying levels of security. For instance, the more critical zones may require 3-factor authentication where the open area may only require normal access controls. This type of approach requires a solid understanding of an agency's information and data types gained through the security categorization process.

[21] FEA Consolidated Reference Model Document Version 2.3, October 2007

- Contingency and Disaster Recovery Planning: Contingency and disaster recovery planning personnel should review information systems that have multiple data types of varying impact levels and consider grouping applications with similar information system impact levels with sufficiently protected infrastructures. This ensures efficient application of the correct contingency and disaster protection security controls and avoids the over protection of lower impact information systems.
- Information Sharing and System Interconnection Agreements: Agency personnel should utilize aggregated and individual security categorization information when assessing interagency connections. For example, knowing that information processed on a high impact information system is flowing to another agency's moderate impact information system should cause both agencies to evaluate the security categorization information, the implemented or resulting security controls, and the risk associated with interconnecting systems. The results of this evaluation may substantiate the need for additional security controls in the form of a Service Level Agreement, information systems upgrades, additional mitigating security controls, or alternative means of sharing the required information.

APPENDIX A: GLOSSARY OF TERMS

Accreditation

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. [FIPS 200, NIST SP 800-37]

Accreditation Boundary

All components of an information system to be accredited by an authorizing official and excludes separately accredited systems to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3. [NIST SP 800-37]

Accrediting Authority

See Authorizing Official.

Agency

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. [41 U.S.C., Sec. 403]

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. [FIPS 200]

Authenticity

The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See authentication.

Authorizing Official

Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Synonymous with Accreditation Authority. [FIPS 200, NIST SP 800-37]

Availability

Ensuring timely and reliable access to and use of information. [44 U.S.C., Sec. 3542]

Business Areas

"Business areas" separate government operations into high-level categories relating to the purpose of government, the mechanisms the government uses to achieve its purposes, the support functions necessary to conduct government operations, and resource management functions that support all areas of the government's business. "Business areas" are subdivided into "areas of operation" or "lines of business." The recommended information types provided in NIST SP 800-60 are established from the "business areas" and "lines of business" from OMB's Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

Certification

A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. [FIPS 200, NIST SP 800-37]

Chief Information Officer

Agency official responsible for:
(i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency;
(ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and
(iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. [PL 104-106, Sec. 5125(b)]

Classified Information

Information that has been determined pursuant to Executive Order (E.O.) 13292 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Command and Control

The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., Sec. 3542]

Counterintelligence

Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities.

Criticality

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

Cryptologic

Of or pertaining to cryptology.

Cryptology

The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.

Executive Agency

An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec.102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); or a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. [41 U.S.C., Sec. 403]

Federal Enterprise Architecture
[FEA Program Management Office]

A business-based framework for government-wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.

Federal Information System

An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. [40 U.S.C., Sec. 11331]

General Support System

An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. [OMB Circular A-130, Appendix III]

High-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high. [FIPS 200]

Impact

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Independent Regulatory Agency

The Board of Governors of the Federal Reserve System, the Commodity Futures Trading Commission, the Consumer Product Safety Commission, the Federal Communications Commission, the Federal Deposit Insurance Corporation, the Federal Energy Regulatory Commission, the Federal Housing Finance Board, the Federal Maritime Commission, the Federal Trade Commission, the Interstate Commerce Commission, the Mine Enforcement Safety and Health Review Commission, the National Labor Relations Board, the Nuclear Regulatory Commission, the Occupational Safety and Health Review Commission, the Postal Rate Commission, the Securities and Exchange Commission, and any other similar agency designated by statute as a Federal independent regulatory agency or commission.

Individual

A citizen of the United States or an alien lawfully admitted for permanent residence. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.

Information

An instance of an information type. [FIPS 199]

Information Owner

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. [CNSS Inst. 4009]

Information Resources

Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., Sec. 3502]

Information Security

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., Sec. 3542]

Information System

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., Sec. 3502; OMB Circular A-130, Appendix III]

Information System Owner (or Program Manager)

Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [CNSS Inst. 4009, Adapted]

Information System Security Officer

Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or information system owner for maintaining the appropriate operational security posture for an information system or program. [CNSS Inst. 4009, Adapted]

Information Technology

Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. [40 U.S.C., Sec. 1401]

Information Type

A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation. [FIPS 199]

Integrity

Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]

Intelligence

(i) the product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas; or

(ii) information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. The term 'intelligence' includes foreign intelligence and counterintelligence.

Intelligence Activities

The term 'intelligence activities' includes all activities that agencies within the Intelligence Community are authorized to conduct pursuant to Executive Order 12333, United States Intelligence Activities.

Intelligence Community

The term 'intelligence community' refers to the following agencies or organizations:

(i) The Central Intelligence Agency (CIA);
(ii) The National Security Agency (NSA);
(iii) The Defense Intelligence Agency (DIA);
(iv) The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;
(v) The Bureau of Intelligence and Research of the Department of State;
(vi) The intelligence elements of the Army, Navy, Air Force, and Marine Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; and
(vii) The staff elements of the Director of Central Intelligence.

Lines of Business

“Lines of business” or “areas of operation” describe the purpose of government in functional terms or describe the support functions that the government must conduct in order to effectively deliver services to citizens. *Lines of business* relating to the purpose of government and the mechanisms the government uses to achieve its purposes tend to be mission-based. *Lines of business* relating to support functions and resource management functions that are necessary to conduct government operations tend to be common to most agencies. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

Low-Impact System

An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low. [FIPS 200]

Mission Critical

Any telecommunications or information system that is defined as a *national security system* (FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of an agency.

Moderate-Impact System

An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate and no security objective is assigned a FIPS 199 potential impact value of high. [FIPS 200]

National Security Information

Information that has been determined pursuant to Executive Order 12958 as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.

National Security System

Any information system (including any telecommunications system) used or operated by an agency or by a contractor on behalf of an agency, or any other organization on behalf of an agency –

(i) the function, operation, or use of which: involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapon system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example payroll, finance, logistics, and personnel management applications); or

(ii) is protected at all times by procedures established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. [44 U.S.C., Sec. 3542]

Non-repudiation

Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information. [CNSS Inst. 4009 Adapted]

Potential Impact

The loss of confidentiality, integrity, or availability could be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals. [FIPS 199]

Privacy Impact Assessment (PIA)

An analysis of how information is handled:

(i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy;

(ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and

(iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. [OMB Memorandum 03-22]

Public Information

Any information, regardless of form or format that an agency discloses, disseminates, or makes available to the public.

Risk

The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [FIPS 200, Adapted]

Security Category

The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, or the Nation. [FIPS 199, Adapted]

Security Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [FIPS 199]

Security Objectives

Confidentiality, integrity, and availability.[FIPS 199]

Senior Agency Information Security Officer

Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. [44 U.S.C., Sec. 3544]

Sensitivity

Used in this guideline to mean a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

Sub-functions

Sub-functions are the basic operations employed to provide the system services within each area of operations or line of business. The recommended information types provided in NIST SP 800-60 are established from the “business areas” and “lines of business” from OMB’s Business Reference Model (BRM) section of *Federal Enterprise Architecture (FEA) Consolidated Reference Model Document Version 2.3*

System

See Information System.

Telecommunications

The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received.

Threat

Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. [CNSS Inst. 4009, Adapted]

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSS Inst. 4009, Adapted]

Weapons System

A combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery and deployment (if applicable) required for self-sufficiency.

APPENDIX B: REFERENCES

S. 3418 [5 U.S.C. § 552A through Public Law 93-579], 93rd U.S. Cong., 2d Sess., *The Privacy Act of 1974,* December 31, 1974 (effective September 27, 1975).

S. 244 [Public Law 104-13], 104th U.S. Cong., 1t Sess., *Paperwork Reduction Act of 1995*, May 22, 1995.

S. 1124, Division E [Public Law 104-106], 104th U.S. Cong., 2d Sess., *Information Technology Management Reform Act of 1996,* February 10, 1996.

H.R. 3162, Titles VII and Title IX [Public Law 107-56], 107th U.S. Cong., 1t Sess., *The USA PATRIOT Act of 2001,* October 26, 2001.

Public Law 107-296, *Critical Information Infrastructure Act of 2002*, §§211-215, November 25, 2002.

H.R. 2458 [Public Law 107-347], 107th U.S. Cong., 2d Sess., *E-Government Act of 2002*, December 17, 2002.

H.R. 2458, Title III [Public Law 107-347], 107th U.S. Cong., 2d Sess., *Federal Information Security Management Act of 2002,* December 17, 2002.

Executive Office of the President, *Presidential Decision Directive 63, Protecting America's Critical Infrastructures,* May 22, 1998.

United States Office of Management and Budget, Circular No. A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.

United States Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 29, 2003.

United States Office of Management and Budget (OMB), Federal Enterprise Architecture (FEA) Program Management Office (PMO), *FEA Consolidated Reference Model 2.3*, October 2007.

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003.

United States Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-18, *Guide for Developing Security Plans for Federal Information Systems*, Revision 1, February 2006.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-39, *Draft Managing Risk from Information Systems: An Organizational Perspective*, April 2008.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, Revision 2, December 2007.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems,* July 2008.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

United States Department of Commerce, National Institute of Standards and Technology, Special Publication 800-64, *Security Considerations in the Information System Development Life Cycle,* June 2004.

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

May 22, 2007

M-07-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Safeguarding personally identifiable information[1] in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA)[2] and the Privacy Act of 1974.[3]

As part of the work of the Identity Theft Task Force,[4] this memorandum requires agencies to develop and implement a breach[5] notification policy[6] **within 120 days**. The attachments to this memorandum outline the framework within which agencies must develop this breach notification policy[7] while ensuring proper safeguards are in place to protect the information. Agencies should

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

[2] Title III of the E-Government Act of 2002, Pub. L. No. 107-347.

[3] 5 U.S.C. § 552a.

[4] Executive Order 13402 charged the Identity Theft Task Force with developing a comprehensive strategic plan for steps the federal government can take to combat identity theft, and recommending actions which can be taken by the public and private sectors. On April 23, 2007 the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov.

[5] For the purposes of this policy, the term "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

[6] Agencies should use a best judgment standard to develop and implement a breach notification policy. Using a best judgment standard, the sensitivity of certain terms, such as personally identifiable information, can be determined in context. For example, an office rolodex contains personally identifiable information (name, phone number, etc.). In this context the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease probably would be considered sensitive information. Similarly, using a best judgment standard, discarding a document with the author's name on the front (and no other personally identifiable information) into an office trashcan likely would not warrant notification to US-CERT.

[7] Terms not specifically defined within this Memorandum (*e.g.*, sensitive) should be considered to reflect the definition found in a commonly accepted dictionary.

note the privacy and security requirements addressed in this Memorandum apply to all Federal information and information systems.[8] Breaches subject to notification requirements include both electronic systems as well as paper documents. In short, agencies are required to report on the security of information systems in any formant (*e.g.*, paper, electronic, etc.). [9]

In formulating a breach notification policy, agencies must review their existing requirements with respect to Privacy and Security (see Attachment 1). The policy must include existing and new requirements for Incident Reporting and Handling (see Attachment 2) as well as External Breach Notification (see Attachment 3). Finally, this document requires agencies to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information (see Attachment 4).

Within the framework set forth in the attachments, agencies may implement more stringent policies and procedures reflecting the mission of the agency. While this framework identifies a number of steps to greatly reduce the risks related to a data breach of personally identifiable information, it is important to emphasize that a few simple and cost-effective steps may well deliver the greatest benefit, such as:

- reducing the volume of collected and retained information to the minimum necessary;
- limiting access[10] to only those individuals who must have such access; and
- using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

This Memorandum should receive the widest possible distribution within your agency and each affected organization and individual should understand their specific responsibilities for implementing the procedures and requirements. Materials created in response to this Memorandum and attachments should be made available to the public through means determined by the agency, *e.g.*, posted on the agency web site, by request, etc.

Consistent with longstanding policy requiring agencies to incorporate the costs for securing their information systems, all costs of implementing this memorandum, including development,

[8] FISMA security requirements apply to Federal information and information systems, including both paper and electronic format.

[9] A plan to review the controls for information systems not previously included in other security reviews must be addressed in the agency's breach notification policy (*e.g.*, timeframe for completion of review, etc.); however, completion of the review for those systems is not required to be finished within the 120-day timeframe for development of the policy.

[10] In this policy, “access” means the ability or opportunity to gain knowledge of personally identifiable information.

implementation, notification to affected individuals, and any remediation activities, will be addressed through existing agency resources of the agency experiencing the breach.

Because of the many alternate ways to implement a risk-based program within the framework provided, this Memorandum, or its attachments, should not be read to mean an agency's failure to implement one or more of the many security provisions discussed within[11] would constitute less than adequate protections required by the Privacy Act. These new requirements do not create any rights or benefits, substantive or procedural, which are enforceable at law against the government.

Questions about this Memorandum should be directed to Hillary Jaffe of my staff at hjaffe@omb.eop.gov.

Attachments

[11] For example, FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST).

Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information

This Attachment reemphasizes the responsibilities under existing law, executive orders, regulations, and policy to appropriately safeguard personally identifiable information and train employees on responsibilities in this area (Section A).[12] It also establishes two new privacy requirements and discusses five security requirements as described below (Sections B and C).

A. Current Requirements

1. Privacy Act Requirements. In particular, the Privacy Act of 1974 (Privacy Act)[13] requires each agency to:

a. Establish Rules of Conduct. Agencies are required to establish "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance." (5 U.S.C. § 552a(e)(9))

b. Establish Safeguards. Agencies are also required to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained." [14]

c. Maintain accurate, relevant, timely and complete information. The Privacy Act also requires personally identifiable information within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete including through the use of notices to the public.[15] It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and

[12] This Memorandum, or its attachments, should not be read to mean an agency's failure to implement one or more of the many provisions of FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST) would constitute less than adequate protections required by the Privacy Act of 1974.

[13] 5 U.S.C. § 552a.

[14] 5 U.S.C. § 552a (e)(10).

[15] The Privacy Act requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination" in their systems of records. 5 U.S.C. § 552a(e)(5).

OMB's implementing policies.[16] By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it.

2. Security Requirements.

Below are four particularly important existing security requirements agencies already should be implementing:

a. Assign an impact level to all information and information systems. Agencies must follow the processes outlined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize all information and information systems according to the standard's three levels of impact (*i.e.*, low, moderate, or high). Agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

b. Implement minimum security requirements and controls. For each of the impact levels identified above, agencies must implement the minimum security requirements and minimum (baseline) security controls set forth in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, respectively.

c. Certify and accredit information systems. Agencies must certify and accredit (C&A) all information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[17] The specific procedures for conducting C&A are set out in NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and include guidance for continuous monitoring of certain security controls. Agencies' continuous monitoring should assess a subset of the management, operational, and technical controls used to safeguard such information (*e.g.*, Privacy Impact Assessments).

d. Train employees. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to

[14] The Privacy Act requires agencies to publish a notice of any new or intended use of information maintained in a system of records in the Federal Register to provide an opportunity for the public to submit comments. 5 U.S.C. § 552a(e)(4). Agencies are also required to publish notice of any subsequent substantive revisions to the use of information maintained in the system of records. 5 U.S.C. § 552a(e)(11). OMB Circular A-130 ("Management of Federal Information Resources") offers additional guidance on this issue. OMB Circular A-130, App. I, sec. 4.c.

[17] 44 U.S.C. 3544(b).

ensure employees continue to understand their responsibilities.[18] Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing tele-work and other authorized remote access programs, training must also include the rules of such programs.[19]

B. Privacy Requirements

1. Review and Reduce the Volume of Personally Identifiable Information.

a. Review Current Holdings. Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.[20] Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual report under FISMA.

Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act systems of records notices.

To help safeguard personally identifiable information, agencies are reminded they must meet the requirements of FISMA and associated policies and guidance from the OMB and NIST.[21] FISMA requires each agency to implement a comprehensive security program to protect the agency's information and information systems; agency Inspectors General must independently evaluate the agency's program; and agencies must report annually to OMB and Congress on the effectiveness of their program.

[18] Agencies may schedule training to coincide with existing activities, such as ethics training. Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. The Department of Defense, the Office of Personnel Management, and the Department of State offer agencies a minimum baseline of security awareness training as part of the Information Systems Security Line of Business.

[19] Agencies should also consider augmenting their training by using creative methods to promote daily awareness of employees' privacy and security responsibilities, such as weekly tips, mouse pads imprinted with key security reminders, privacy screens for public use of laptops, and incentives for reporting security risks.

[20] To the extent agencies are substantively performing these reviews, agencies should leverage these efforts to meet the new privacy requirements. This provision does not apply to apply to the accessioned holdings (archival records) held by the National Archives and Records Administration (NARA).

[21] The Department of Defense and Intelligence Community establish their own policy and guidance for the security of their information systems. 44 U.S.C. 3543(c).

Within the above framework, agencies may implement more stringent procedures governed by specific laws, regulations, and agency procedures to protect certain information, for example, taxpayer data, census information, and other information.

2. Reduce the Use of Social Security Numbers.

a. Eliminate Unnecessary Use. Agencies must now also review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months.[22]

b. Explore Alternatives. Agencies must participate in government-wide efforts to explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs (*e.g.*, surveys, data calls, etc.).

C. Security Requirements

While agencies continue to be responsible for implementing all requirements of law and policy, below are five requirements[23] agencies must implement which derive from existing security policy and NIST guidance. These requirements are applicable to all Federal information, *e.g.*, law enforcement information, etc.

- Encryption. Encrypt, using only NIST certified cryptographic modules, [24] all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary[25] or a senior-level individual he/she may designate in writing;
- Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Time-Out Function. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity;
- Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required; and

[22] Agencies with questions addressing this assignment regarding the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq*.) should contact their respective desk officer at the Office of Management and Budget.

[23] See OMB Memo 06-16 "Protection of Sensitive Agency Information" (www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf).

[24] See NIST's website at http://csrc.nist.gov/cryptval/ for a discussion of the certified encryption products.

[25] Non cabinet agencies should consult the equivalent of a Deputy Secretary.

- Ensure Understanding of Responsibilities. Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities.

Agencies should also contemplate and incorporate best practices to prevent data breaches. Examples of such practices might include using privacy screens when working outside the office or requiring employees to include laptop computers in carry-on luggage rather than checked baggage.

Attachment 2: Incident Reporting and Handling Requirements

This Attachment applies to security incidents involving the breach of personally identifiable information whether in electronic or paper format. For the purposes of reporting, agencies must continue to follow existing requirements, as modified and described below.

A. Existing Requirements

1. FISMA Requirements. FISMA requires each agency to:

- implement procedures for detecting, reporting and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done
- notify and consult with:
    - the Federal information security incident center
    - law enforcement agencies and Inspectors General
    - an office designated by the President for any incident involving a national security system
    - any other agency or office in accordance with law or as directed by the President.[26]
- implement NIST guidance and standards[27]

Federal Information Processing Standards Publication 200 (FIPS 200) and NIST Special Publication 800-53 provide a framework for categorizing information and information systems, and provide minimum security requirements and minimum (baseline) security controls for incident handling and reporting. The procedures agencies must already use to implement the above FISMA requirements are found in two primary guidance documents: NIST Special Publication 800-61, *Computer Security Incident Handling Guide*[28]; and the concept of operations for the Federal security incident handling center located within the Department of Homeland Security, *i.e.*, United States Computer Emergency Readiness Team (US-CERT).[29]

[26] 44 U.S.C. § 3544(b)(7).

[27] For additional information on NIST guidance and standards, see www.nist.gov.

[28] See "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology" (http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf).

[29] The responsibilities of US-CERT are outlined in 44 U.S.C. § 3546. Its complete set of operating procedures may be found on the US-CERT website **(**www.us-cert.gov/federal/reportingRequirements.html). Separate procedures are in place for the Department of Defense as identified in Directive O-8530-1 and all components report incidents to the Joint Task Force Global Network Operations (JTF-GNO), which, in turn, coordinates directly with the US-CERT.

2. Incident Handling and Response Mechanisms. When faced with a security incident, an agency must be able to respond in a manner protecting both its own information and helping to protect the information of others who might be affected by the incident. To address this need, agencies must establish formal incident response mechanisms. To be fully effective, incident handling and response must also include sharing information concerning common vulnerabilities and threats with those operating other systems and in other agencies. In addition to training employees on how to prevent incidents, all employees must also be instructed in their roles and responsibilities regarding responding to incidents should they occur.

B. Modified Agency Reporting Requirements

1. US-CERT Modification. Agencies must report all incidents involving personally identifiable information to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches. The US-CERT concept of operations for reporting Category 1 incidents is modified as follows:

> Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information. In this category agencies must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred. Reporting to US-CERT is required within one hour of discovery/detection.

- For incidents involving personally identifiable information, agencies must:
  - Continue to follow internal agency procedures for notifying agency officials including your agency privacy official and Inspector General;
  - Notify the issuing bank if the breach involves government-authorized credit cards; and
  - Notify US-CERT within one hour. Although only limited information about the breach may be available, US-CERT must be advised so it can assist in coordinating communications with the other agencies. Updates should be provided as further information is obtained.
- Under specific procedures established for these purposes, after notification by an agency, US-CERT will notify the appropriate officials.
- Monthly, US-CERT will distribute to designated officials in the agencies and elsewhere, a report identifying the number of confirmed breaches of personally identifiable information and will also make available a public version of the report.

2. Develop and Publish a Routine Use.

a. Effective Response. A federal agency's ability to respond quickly and effectively in the event of a breach of federal data is critical to its efforts to prevent or minimize any consequent harm.[30] An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

b. Disclosure of Information. Often, the information to be disclosed to such persons and entities is maintained by federal agencies and is subject to the Privacy Act (5 U.S.C. § 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory exceptions.31 In order to ensure an agency is in the best position to respond in a timely and effective manner, in accordance with 5 U.S.C. § 552a(b)(3) of the Privacy Act, agencies should publish a routine use for appropriate systems specifically applying to the disclosure of information in connection with response and remedial efforts in the event of a data breach as follows:

> To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.[32]

As described in the President's Identity Theft Task Force's Strategic Plan, all agencies should publish a routine use for their systems of records allowing for the disclosure of information in the course of responding to a breach of federal data.[33] Such a routine use will serve to protect the interests of the individuals whose information is at issue by allowing agencies to take appropriate steps to facilitate a timely and effective response, thereby improving their ability to prevent, minimize, or remedy any harm resulting from a compromise of data maintained in their systems of records.

[30] Here, "harm" means damage, fiscal damage, or loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.

[31] 5 U.S.C. §§ 552a(b)(1)-(12).

[32] See Appendix B of the Identity Theft Task Force report (www.identitytheft.gov/reports/StrategicPlan.pdf).

[33] *Id.*

Attachment 3: External Breach Notification

To ensure consistency across government, this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification.[34] This Attachment does not attempt to set a specific threshold for external notification since breaches are specific and context dependant and notification is not always necessary or desired. The costs of any notifications must be borne by the agency experiencing the breach from within existing resources.

A. Background

1. Harm. Breaches can implicate a broad range of harms to individuals, including the potential for identity theft; however, this Section does not discuss actions to address possible identity theft or fraud. Agencies are referred to the ID Theft Task Force's Strategic Plan for guidance.

2. Requirement. Agencies must implement the one specific new requirement discussed below; *i.e.*, develop a breach notification policy and plan (see Section B. below).

3. Threshold questions. Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require agencies to resolve a number of threshold questions.[35] The likely risk of harm and the level of impact will determine when, what, how and to whom notification should be given.[36]

Notification of those affected and/or the public allows those individuals the opportunity to take steps to help protect themselves from the consequences of the breach. Such notification is also consistent with the "openness principle" of the Privacy Act that calls for agencies to inform individuals about how their information is being accessed and used, and may help individuals mitigate the potential harms resulting from a breach.

4. Chilling Effects of Notices. A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public.[37] In addition, agencies should

[34] These factors do not apply to an agency's notification to US-CERT. Agencies must report all incidents – potential and confirmed – involving personally identifiable information to US-CERT.

[35] Notice may not be necessary if, for example, the information is properly encrypted because the information would be unusable.

[36] See OMB's September 20, 2006 memorandum titled "Recommendations for Identity Theft Related Data Breach Notification" for information and recommendations for planning and responding to data breaches which could result in identity theft (www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

[37] Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft* (Washington, D.C.: June 16, 2005), p. 10. In this testimony, the Federal Trade Commission raised concerns about the threshold for which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects.

consider the costs to individuals and businesses of responding to notices where the risk of harm may be low. Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.

B. New Requirement

Each agency should develop a breach notification policy and plan comprising the elements discussed in this Attachment. In implementing the policy and plan, the Agency Head will make final decisions regarding breach notification.

Six elements should be addressed in the policy and plan and when considering external notification:

- whether breach notification is required
- timeliness of the notification
- source of the notification
- contents of the notification
- means of providing the notification
- who receives notification: public outreach in response to a breach

To ensure adequate coverage and implementation of the plan, each agency should establish an agency response team including the Program Manager of the program experiencing the breach, Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy, Communications Office, Legislative Affairs Office, General Counsel and the Management Office which includes Budget and Procurement functions.[38] A more detailed description of these elements is set forth below:

1. Whether Breach Notification is Required

To determine whether notification of a breach is required, the agency should first assess the likely risk of harm caused by the breach and then assess the level of risk. Agencies should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach.[39] Agencies should bear in mind that notification when there is little or no risk of harm might create

[38] Non-Cabinet-level agencies should include their functional equivalent.

[39] For reference, the express language of the Privacy Act requires agencies to consider a wide range of harms: agencies shall "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a (e)(10).

unnecessary concern and confusion.[40] Additionally, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

Five factors should be considered to assess the likely risk of harm:

a. Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals.[41] It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context.[42] In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

b. Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the determining factor for whether an agency should provide notification.

c. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed by the agency. (See Attachment 1 above.) If the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent.[43]

Agencies will first need to assess whether the personally identifiable information is at a low, moderate, or high risk of being compromised. The assessment should be guided by NIST

[40] Another consideration is a surfeit of notices, resulting from notification criteria which are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant.

[41] For example, theft of a database containing individuals' names in conjunction with Social Security numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.

[42] For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.

[43] In this context, proper protection means encryption has been validated by NIST.

security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

d. Likelihood the Breach May Lead to Harm

1. Broad Reach of Potential Harm. The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[44] Additionally, agencies should consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

2. Likelihood Harm Will Occur. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force.[45]

e. Ability of the Agency to Mitigate the Risk of Harm. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken.[46] Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

[44] 5 U.S.C. § 552a(e)(10).

[45] See "Recommendations for Identity Theft Related Data Breach Notification" (www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

[46] For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

2. Timeliness of the Notification

Agencies should provide notification without unreasonable delay following the discovery of a breach, consistent with the needs of law enforcement and national security and any measures necessary for your agency to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised.

Decisions to delay notification should be made by the Agency Head or a senior-level individual he/she may designate in writing. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s).

3. Source of the Notification

In general, notification to individuals affected by the breach should be issued by the Agency Head, or senior-level individual he/she may designate in writing, or, in those instances where the breach involves a publicly known component of an agency, such as the Food and Drug Administration or the Transportation Security Administration, the Component Head. This demonstrates it has the attention of the chief executive of the organization. Notification involving only a limited number of individuals (*e.g.*, under 50) may also be issued jointly under the auspices of the Chief Information Officer and the Chief Privacy Officer or Senior Agency Official for Privacy. This approach signals the agency recognizes both the security and privacy concerns raised by the breach.

When the breach involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, the agency is responsible for ensuring any notification and corrective actions are taken. The roles, responsibilities, and relationships with contractors or partners should be reflected in your breach notification policy and plan, your system certification and accreditation documentation, and contracts and other documents.

4. Contents of the Notification

The notification should be provided in writing and should be concise, conspicuous, plain language. The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;

- To the extent possible, a description of the types of personal information involved in the breach (*e.g.*, full name, Social Security number, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system;
- What steps individuals should take to protect themselves from potential harm, if any;
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- Who affected individuals should contact at the agency for more information, including a toll-free telephone number, e-mail address, and postal address.

Given the amount of information required above, you may want to consider layering the information as suggested in Section 5 below, providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on your web site. If you have knowledge the affected individuals are not English speaking, notice should also be provided in the appropriate language(s). You may seek additional guidance on how to draft the notice from the Federal Trade Commission, a leader in providing clear and understandable notices to consumers, as well as from communication experts who may assist you in designing model notices.[47] A standard notice should be part of your approved breach plan.

5. Means of Providing Notification

The best means for providing notification will depend on the number of individuals affected and what contact information is available about the affected individuals. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following examples are types of notice which may be considered.

a. Telephone. Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

[47] Additional guidance on how to draft a notice is available in the FTC publication titled “Dealing with a Data Breach” (www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html). Although the brochure is designed for private sector entities that have experienced a breach, it contains sample notice letters that could also serve as a model for federal agencies. You may also seek guidance from communications experts who may assist you in designing model notices.

b. First-Class Mail. First-class mail notification to the last known mailing address of the individual in your agency's records should be the primary means notification is provided. Where you have reason to believe the address is no longer current, you should take reasonable steps to update the address by consulting with other agencies such as the US Postal Service. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If the agency which experienced the breach uses another agency to facilitate mailing (for example, if the agency which suffered the loss consults the Internal Revenue Service for current mailing addresses of affected individuals), care should be taken to ensure the agency which suffered the loss is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents, *e.g.*, "Data Breach Information Enclosed" and should be marked with the name of your agency as the sender to reduce the likelihood the recipient thinks it is advertising mail.

c. E-Mail. E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where an individual has provided an e-mail address to you and has expressly given consent to e-mail as the primary means of communication with your agency, and no known mailing address is available, notification by e-mail may be appropriate. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the agency and www.USA.gov[48] web sites, where the notice may be "layered" so the most important summary facts are up front with additional information provided under link headings.

d. Existing Government Wide Services. Agencies should use Government wide services already in place to provide support services needed, such as USA Services, including toll free number of 1-800-FedInfo and www.USA.gov.

e. Newspapers or other Public Media Outlets. Additionally, you may supplement individual notification with placing notifications in newspapers or other public media outlets. You should also set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

f. Substitute Notice. Substitute notice in those instances where your agency does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the home page of your agency's web site and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

[48] The current domain name for the Federal Internet portal required by section 204 of the E-Government Act of 2002 is www.usa.gov.

g. Accommodations. Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the agency web site.

6. Who Receives Notification: Public Outreach in Response to a Breach

a. Notification of Individuals. The final consideration in the notification process when providing notice is to whom you should provide notification: the affected individuals, the public media, and/or other third parties affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification.

b. Notification of Third Parties including the Media. If communicating with third parties regarding a breach, agencies should consider the following.

1. *Careful Planning.* An agency's decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies as described above in Section 2. To the extent possible, when necessary prompt public media disclosure is generally preferable because delayed notification may erode public trust.

2. *Web Posting.* Agencies should post information about the breach and notification in a clearly identifiable location on the home page of your agency web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. The posting should include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process.[49] The information should also appear on the www.USA.gov web site. You may also consult with GSA's USA Services regarding using their call center.

3. *Notification of other Public and Private Sector Agencies.* Other public and private sector agencies may need to be notified on a need to know basis, particularly those that may be

[49] See the FAQ posted by the Department of Veterans Affairs in response to the May 2006 incident for examples of links to identity theft resources and a sample FAQ (www.usa.gov/veteransinfo.shtml).

affected by the breach or may play a role in mitigating the potential harms stemming from the breach.[50]

4. Congressional Inquiries. Agencies should be prepared to respond to inquires from other governmental agencies such as the Government Accountability Office and Congress.

c. Reassess the Level of Impact Assigned to the Information. After evaluating each of these factors, you should review and reassess the level of impact you have already assigned to the information using the impact levels defined by the NIST.[51] The impact levels – low, moderate, and high, describe the (worst case) potential impact on an organization or individual if a breach of security occurs.[52]

- **Low:** the loss of confidentiality, integrity, or availability is expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals
- **Moderate:** the loss of confidentiality, integrity, or availability is expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals.
- **High:** the loss of confidentiality, integrity, or availability is expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets or individuals.

The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm. If agencies appropriately apply the five risk factors discussed in section 1 of this attachment within the fact-specific context, it is likely notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification.

[50] For example, a breach involving medical information may warrant notification of the breach to health care providers and insurers through the public or specialized health media, and a breach of financial information may warrant notification to financial institutions through the federal banking agencies.

[51] See FIPS 199 and Attachment 1 of this memorandum. Reassessment is suggested as the context of any breach may alter your original designation.

[52] The determination of the potential impact of loss of information is made by the agency during an information system's certification and accreditation process.

Attachment 4: Rules and Consequences

A. New Requirement: Rules and Consequences Policy.

Fairness requires that managers, supervisors and employees be informed and trained regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities. Therefore, it is the responsibility of each agency head to develop and implement an appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available for failure to follow these rules. Consequences should be commensurate with level of responsibility and type of personally identifiable information involved. Supervisors also must be reminded of their responsibility to instruct, train and supervise employees on safeguarding personally identifiable information. Agencies should develop and implement these policies in accordance with the agency's respective existing authorities.

As with any disciplinary action, the particular facts and circumstances, including whether the breach was intentional, will be considered in taking appropriate action. Supervisors also should be reminded that any action taken must be consistent with law, regulation, applicable case law, and any relevant collective bargaining agreement. Supervisors should understand they may be subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take required steps to prevent a breach from occurring.

Agencies having questions regarding development of a rules and consequences policy may contact OPM’s Center for Workforce Relations and Accountability Policy at (202) 606-2930.

1. Affected Individuals. At a minimum, each agency should have a documented policy in place which applies to employees of the agency (including managers), and its contractors, licensees, certificate holders, and grantees.

2. Affected Actions. The agency’s policy should describe the terms and conditions affected individuals shall be subject to and identify available corrective actions. Rules of behavior and corrective actions should address the following:

- Failure to implement and maintain security controls, for which an employee is responsible and aware, for personally identifiable information regardless of whether such action results in the loss of control[53] or unauthorized disclosure of personally identifiable information;

[53] Here, “control” means the authority of the government agency that originates information, or its successor in function, to regulate access to the information. Having control is a condition or state and not an event. Loss of control is also a condition or state which may or may not lead to an event, *i.e.*, a breach.

- Exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable information;
- Failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information; and
- For managers, failure to adequately instruct, train, or supervise employees in their responsibilities.

3. Consequences. Applicable consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy. The minimum consequence agencies should consider is prompt removal of authority to access information or systems from individuals who demonstrates egregious disregard or a pattern of error in safeguarding personally identifiable information.

International Privacy-Session 304

Useful Websites/Links

1. DLA Piper Global Privacy Desk Reference:

   http://www.dlapiper.com/us/publications/detail.aspx?pub=2362

2. Morrison & Forrester Privacy Library:

   http://www.mofo.com/privacy--data-security-services/

3. Department of Commerce EU-US Safe Harbor:

   http://www.export.gov/safeharbor/index.asp

4. European Commission Data Protection Webpage:

   http://ec.europa.eu/justice/policies/privacy/index_en.htm

5. ACC Virtual Library:

   http://www.acc.com/legalresources/publications/infopaklistings.cfm

   Including the following **InfoPaks**:

   Doing Business Internationally

   E-Commerce Legal Primer

   Homeland Security

   Email & Internet Policies

ACC – International Privacy--

Issues Contained in Fact Pattern for 1836 Technologies, Inc.

1. What is Personally Identifiable Information, Data Privacy, and how can you determine whether your company has PII and/or Sensitive Data; and how do you handle/protect/use PII or Personal Data?

2. What laws are applicable to monitoring Employees' use of computers, Internet activity, and e-mail in the United States and ROW (e.g., Europe, Australia, Canada, etc.), and what are the differences between the US and Europe vis-à-vis consent to such monitoring activities?

3. With respect to government contractors what Federal Law(s) apply to/regulate notice of intrusion into the Company's computer networks (e.g., DoD, SEC, Banking regulations)?

4. What is NIST, and what NIST Standards, OMB Circulars, and DoD Directives apply to PII, Network security and when and how do they apply to government contractors and their employees?

5. What are the different laws that apply to data breach notification to affected individuals that their PII may have been compromised (employees, third parties, and veterans) (Federal EU, and State laws), and what types of remediation may be legally mandated by various jurisdictions?

6. What, if any, laws may apply (or prohibit) the retention of a Canadian entity to handle credit reporting service (transfer of information to Canadian entity – from the US, Europe and ROW);

7. What issues are raised by the text contained in the Letter to affected individuals? Who must it go to? By when? What are implications?

8. How reconcile various federal, state, and EU related laws? What is the best approach for the company to take? How coordinate?

9 What privacy issues are created by hosting the servers in the US for 1836 with regard to its employees located in the UE, India, etc.? How mitigate them?

10. What privacy related issues are created as a result of 1836's practice of backing up the Servers and e-mail files and storing them in its off-site repository in Grand Rapids?

11. What privacy issues are created by operating the IT Solutions Department out of India?

ACC – International Privacy--

Issues Contained in Fact Pattern for 1836 Technologies, Inc.

12. As a Government Contractor is 1836 supposed to have an Incident Response Plan in place? What are the elements to an Incident Response Plan? What are some best practices with respect to an Incident Response Team?

13. Review various policies listed in the Fact Pattern.

    i. What are the elements of a Banner notifying employees of "No Privacy: in use of Company Computer";
    ii. What are the issues created in a Company Internet/e-mail Monitoring Policy – differences between US and English versions (e.g., what type of consent will be required?); and
    iii. Appropriate Use of Network and IT Assets – best practices regarding use of USB sticks, accessing unsecure Wi-Fi networks (cafes, airports, hotel lobbies); and 3rd party access to company network;

14. What are the elements of a Corporate Investigation (US and ROW), and privacy related issues that may arise/need to be considered when performing such an investigation?

15. What are some of the unique issues created by the fact that 1836 is a publicly traded company? For instance, can 1836 implement a Whistleblower/hotline in the EU to comply with SOX requirements; and if so, what procedural requirements will it have to meet under the EU directive and nation states; and

16. What are some of the legal and regulatory issues may arise out these incidents that may impact on 1836's reputation and stock value that could require briefing to the Board?

FACT PATTERN For 1836 Technologies, Inc

Part I – The Company and Background

1836 Technologies, Inc. is a publicly traded company headquartered in San Antonio, TX, USA, trading under the ticker symbol XXX. 1836 Technologies is an IT solutions company, and has operations in Europe (England, France, and Germany), India, Australia, and Canada, as well as the United States.

1836 Technologies is a medium size federal government contractor that supports the Veterans Affairs Agency, with smaller operations outside of the US, where it often sources additional finance, IT, and software resources for its commercial/nongovernmental work.

Because of its work for Veterans Affairs, 1836 Technologies hosts a significant amount of data regarding veterans who have received medical care from the VA on its computers, which often means that it maintains personal data regarding both the Agency's employees, as well as those individuals who utilize the Agency's services. 1836 Technologies has set up its network servers in San Antonio, with backup servers located in Grand Rapids, MI. All Servers are backed up weekly, while e-mail servers are backed up nightly. E-mail servers are located in each local country, but pursuant to its document management policy, these e-mail servers are backed up weekly to the US server farm in Grand Rapids via the company's intranet. All backup tapes are kept for one year and then discarded.

To facilitate ease of access within the company, 1836 Technologies has adopted an open/flat computer network [a flat network is a network in which all stations can reach other without going through any intermediary hardware devices, such as a bridge or router.]. This allows for associates located in its various branch offices to access information/documents and work on cross-functional teams. It has invested in the latest technology, which allows its associates to set up video and web conferences, give multi-media presentations, and access information 24/7 from anywhere in the World via secure VPN connectivity. In addition, because it's internal IT Services group is located in Bangalore, India, it has set up a remote access internet hosting solution that allows the IT staff to remotely access remote servers, as well as their employees' computers to update, repair, and resolve issues.

1836 Technologies has recently purchased and installed **Snort** a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS). Snort's network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

PROPRIETARY AND CONFIDENTIAL – DONOT DISTRIBUTE WITHOUT PERMISSION

1836 Technologies is evaluating which configuration of Snort to use. It comes in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Bill Travis, 1836 Technologies's General Counsel, has recently read an ACC Docket article about data privacy and the EU directive governing data privacy in Europe. He has directed Jim Bowie, 1836 Technologies's Compliance officer, to determine whether 1836 Technologies can become Safe Harbor Compliant, and to work on an updated set of policies regarding personal data and data privacy that will apply to 1836 Technologies's work for the US, as well as its activities in the ROW. Some of these policies include:

a) Information Security Governance Policy
b) Information Security Policy,
c) Network Monitoring policy,
c) Incident Response Plan,
d) Return and/or disposal of IT assets,
e) Backup and restore policy,
f) Appropriate Use of Network and IT assets & Rules of Behavior
g) Social Networking;
h) Cyber Controls (use of peripherals such as: USB's, iPods, and external drives); and
i) Develop rules of behavior for use of company systems, laptops, etc

Part II – the hypothetical

James Bonham, the Director of IT, informs the GC that the Company had recently installed SNORT on the company's network and had been monitoring activity on the network for the past month (that is how they identified the cyber attack). In response, the GC asks if the monitoring was limited to US personnel or the entire network. The IT Director informs the GC that it had been set up to monitor all activity within the network, which would include all personnel both in the US and located outside of the US. He volunteers that his had been done without notification to any employees as they were still in the beta testing phase of the rollout. Finally, he informs the GC that they traced the virus to a remote user, who had been traveling to Freedonia, and had accessed the network via VPN from a computer café in that country's capital.

Dave Crockett, the Director of Security, informs the GC that he has traced the sophisticated cyber-attack against the company back to the Freedonian government "or its proxies". He goes on to inform you that he has spoken 'confidentially' to several of his counter-parts at other government contractors who inform him that their computer networks have been compromised as well. While stopping short of accusing the Freedonian government of responsibility for the attacks, he has confirmed that the internet addresses of the attack correspond to a single foreign entity consisting either of agents of the Freedonian state or proxies thereof. To trace this back any further he would have to hire BlackHat Enterprises to further refine his analysis. He wants to know if he can retain them and how much time he has before they have to report the intrusion and possible breach of their system to the Department of Veteran Affairs.

To add insult to injury, during the course of the investigation, the IT Security Group also determines that a laptop that contained PII data from the Veterans Affairs Agency is missing and unaccounted for. The data was/encrypted, but the "owner" of the laptop had quit without notice and no one can recall if he returned his computer. By Contract with the VA, the company is supposed to notify the government, as well as the individuals impacted that there has been a breach and possible loss of personal data. The CIO has informed the GC that it will take two months to reconstruct the missing tape/hard drive, and identify the individuals whose information was lost/stolen or may have been lost/stolen.

Given the above information, the GC turns his attention to determining who must or should be notified of the breach (veterans, employees, law enforcement, federal regulatory agencies, state agencies, state/national/foreign reporting agencies, third-party vendors, insurers and media). He calls in Sue Dickinson, the Privacy Officer, who has been working feverishly on a notification plan. She informs the GC that so far they have determined that PII and related data was accessed for personnel located in all 50 States, as well as data from England, France, Germany, Australia, India, and Canada. She goes on to nonchalantly mention that Identity Theft Resource Center has reported that 656 data breaches were reported in 2008, exposing more than 35 million records, an increase of 47 percent from 2007. Those numbers rose to more than 222 million records exposed in 2009. With a look of dread, she adds that the average cost for responding to a breach was $204 per affected individual in 2009, which seems small until she mentions that there could have been hundreds of thousands of records on the missing computer and an untold number of computer files that may have been accessed.

She informs the GC that she has contacted ExpertPay to provide credit reporting services to all affected employees and government personnel, and has retained ABC TELE Company, a Canadian entity, to set up a call center to deal with the breach. Once approved, she anticipates that it will take at least 2 weeks/days to be operational. To calculate costs, determine the method of communication, and determine eligibility for these services, she asks the GC whether these services will be provided to just US Veterans and US based personnel or if will also be provided to those employees located outside of the USA.

Sue Dickinson, the Privacy Officer, also e-mails a draft of the notice letter for those individuals whose data was on the missing laptop, and asks the GC to review/approve the letter. The letter reads in part:

> "During a routine audit, it has been determined that a laptop computer is unaccounted for. This computer contained personal information, including names, addresses, Social Security numbers and account numbers. We have no reason to believe that anyone has

> accessed or misused your information, but out of an abundance of caution, we have implemented internal monitoring to protect your personal and health information from misuse due to this incident."

The Privacy Officer next informs the GC that there are 46 states, and the District of Columbia, Puerto Rico and the U.S. Virgin Islands, that have data breach notification laws, many with unique requirements. Nuances among the state statutes include that 35 jurisdictions require notification only if there is likely to be a resulting risk of harm, 13 require notice to the applicable attorney general or other state agency, some have specific language to be included in the notification letter, many have requirements about timing of the notice and/or notification to law enforcement before notification to residents, and a handful of states apply their law to both paper and electronic records. Also, depending on the nature of the information and your field, federal laws may apply (although there is no uniform/mandatory federal breach notification law that applies to 1836 Technologies as opposed to the agencies themselves). She also goes on to inform you that under the EU Privacy Directive that there are national laws in Europe that also affect how and what information is protected and whether the company must notify the local Privacy Offices in each country. She understands but is not sure there are similar laws in India, Canada, and Australia.

Samantha Houston, the Information Assurance Office is up next. She informs the GC that the company is supposed to have a first response team in place that includes persons in information technology, information security, compliance, business heads, human resources, legal counsel and public relations/investor relations. Unfortunately, the company had not yet stood up this team, and she is trying to implement the team on the fly. The GC asks her to assign tasks to team members and establish a point person, identify key personnel for each task, calculate timelines and set deadlines, communicate with management and establish attorney-client privilege for investigation and communications. The GC wonders how the government will react to this piece of information.

Finally, the GC calls in Jim Bowie, the now red-faced Compliance officer, who had not yet completed any of the policies that were supposed to be under review and/or implemented. She acknowledges that corporate rules for rigorous control of passwords had not been implemented, or that any training programs had been implemented at 1836 Technologies. He acknowledges that use of uncontrolled USB sticks, 3rd party accessing the company's network, and personnel utilizing unprotected wi-fi spots had been known but not counseled. He also acknowledges that it appeared that IT had been globally gathering data about individuals without their knowledge or permission. E-mail backup tapes and databases of personal information even remotely connected to the Internet had not been properly secured against compromise. The one saving grace is that all lap top computers had been encrypted, so that any information on the laptop, if stolen/lost would be unintelligible – of course if the ex-employee was the culprit, that would be of little solace to the GC or the Company, who decides that he has had enough for one day, and decides to call it a day and go down to the ACC reception and network with his brethren.

PROPOSED FACT SCENARIO

Part I – The Company and Background

1836 Technologies, Inc. is a publicly traded company headquartered in San Antonio, TX, USA, trading under the ticker symbol XXX. 1836 Technologies is an IT solutions company, and has operations in Europe (England, France, and Germany), India, Australia, and Canada, as well as the United States.

1836 Technologies is a medium size federal government contractor that supports the Veterans Affairs Agency, with smaller operations outside of the US, where it often sources additional finance, IT, and Software resources for its commercial/nongovernmental work.

Because of its work for Veterans Affairs, 1836 Technologies hosts a significant amount of data regarding veterans who have received medical care from the VA on its computers, which often means that it maintains personal data regarding both the Agency's employees, as well as those individuals who utilize the Agency's services. 1836 Technologies has set up its network servers in San Antonio, with backup servers located in Grand Rapids, MI. All Servers are backed up weekly, while e-mail servers are backed up nightly. E-mail servers are located in each local country, but pursuant to its document management policy, these e-mail servers are backed up weekly to the US server farm in Grand Rapids via the company's intranet. All backup tapes are kept for one year and then discarded.

To facilitate ease of access within the company, 1836 Technologies has adopted an open/flat computer network [a flat network is a network in which all stations can reach other without going through any intermediary hardware devices, such as a bridge or router.]. This allows for associates located in its various branch offices to access information/documents and work on cross-functional teams. It has invested in the latest technology, which allows its associates to set up video and web conferences, give multi-media presentations, and access information 24/7 from anywhere in the World via secure VPN connectivity. In addition, because it's internal IT Services group is located in Bangalore, India, it has set up a remote access internet hosting solution that allows the IT staff to remotely access remote servers, as well as their employees' computers to update, repair, and resolve issues.

1836 Technologies has recently purchased and installed **Snort** a <u>free</u> and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS). Snort's network-based intrusion detection system (NIDS) has the ability to perform real-time traffic analysis and packet logging on Internet Protocol (IP) networks. The program can also be used to detect probes or attacks, including, but not limited to, operating system fingerprinting attempts, common gateway interface, buffer overflows, server message block probes, and stealth port scans.

PROPRIETARY AND CONFIDENTIAL – DONOT DISTRIBUTE WITHOUT PERMISSION

1836 Technologies is evaluating which configuration of Snort to use. It comes in three main modes: sniffer, packet logger, and network intrusion detection. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the disk. In intrusion detection mode, the program will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

Bill Travis, 1836 Technologies's General Counsel, has recently read an ACC Docket article about data privacy and the EU directive governing data privacy in Europe. He has directed Jim Bowie, 1836 Technologies's Compliance officer, to determine whether 1836 Technologies can become Safe Harbor Compliant, and to work on an updated set of policies regarding personal data and data privacy that will apply to 1836 Technologies's work for the US, as well as its activities in the ROW. Some of these policies include:

a) Information Security Governance Policy
b) Information Security Policy,
c) Network Monitoring policy,
c) Incident Response Plan,
d) Return and/or disposal of IT assets,
e) Backup and restore policy,
f) Appropriate Use of Network and IT assets & Rules of Behavior
g) Social Networking;
h) Cyber Controls (use of peripherals such as: USB's, iPods, and external drives); and
i) Develop rules of behavior for use of company systems, laptops, etc

Part II – the hypothetical

James Bonham, the Director of IT, informs the GC that the Company had recently installed SNORT on the company's network and had been monitoring activity on the network for the past month (that is how they identified the cyber attack). In response, the GC asks if the monitoring was limited to US personnel or the entire network. The IT Director informs the GC that it had been set up to monitor all activity within the network, which would include all personnel both in the US and located outside of the US. He volunteers that his had been done without notification to any employees as they were still in the beta testing phase of the rollout. Finally, he informs the GC that they traced the virus to a remote user, who had been traveling to Freedonia, and had accessed the network via VPN from a computer café in that country's capital.

Dave Crockett, the Director of Security, informs the GC that he has traced the sophisticated cyber-attack against the company back to the Freedonian government "or its proxies". He goes on to inform you that he has spoken 'confidentially' to several of his counter-parts at other government contractors who inform him that their computer networks have been compromised as well. While stopping short of accusing the Freedonian government of responsibility for the attacks, he has confirmed that the internet addresses of the attack correspond to a single foreign entity consisting either of agents of the Freedonian state or proxies thereof. To trace this back any further he would have to hire BlackHat Enterprises to further refine his analysis. He wants to know if he can retain them and how much time he has before they have to report the intrusion and possible breach of their system to the Department of Veteran Affairs.

To add insult to injury, during the course of the investigation, the IT Security Group also determines that a laptop that contained PII data from the Veterans Affairs Agency is missing and unaccounted for. The data was/encrypted, but the "owner" of the laptop had quit without notice and no one can recall if he returned his computer. By Contract with the VA, the company is supposed to notify the government, as well as the individuals impacted that there has been a breach and possible loss of personal data. The CIO has informed the GC that it will take two months to reconstruct the missing tape/hard drive, and identify the individuals whose information was lost/stolen or may have been lost/stolen.

Given the above information, the GC turns his attention to determining who must or should be notified of the breach (veterans, employees, law enforcement, federal regulatory agencies, state agencies, state/national/foreign reporting agencies, third-party vendors, insurers and media). He calls in Sue Dickinson, the Privacy Officer, who has been working feverishly on a notification plan. She informs the GC that so far they have determined that PII and related data was accessed for personnel located in all 50 States, as well as data from England, France, Germany, Australia, India, and Canada. She goes on to nonchalantly mention that Identity Theft Resource Center has reported that 656 data breaches were reported in 2008, exposing more than 35 million records, an increase of 47 percent from 2007. Those numbers rose to more than 222 million records exposed in 2009. With a look of dread, she adds that the average cost for responding to a breach was $204 per affected individual in 2009, which seems small until she mentions that there could have been hundreds of thousands of records on the missing computer and an untold number of computer files that may have been accessed.

She informs the GC that she has contacted ExpertPay to provide credit reporting services to all affected employees and government personnel, and has retained ABC TELE Company, a Canadian entity, to set up a call center to deal with the breach. Once approved, she anticipates that it will take at least 2 weeks/days to be operational. To calculate costs, determine the method of communication, and determine eligibility for these services, she asks the GC whether these services will be provided to just US Veterans and US based personnel or if will also be provided to those employees located outside of the USA.

Sue Dickinson, the Privacy Officer, also e-mails a draft of the notice letter for those individuals whose data was on the missing laptop, and asks the GC to review/approve the letter. The letter reads in part:

> "During a routine audit, it has been determined that a laptop computer is unaccounted for. This computer contained personal information, including names, addresses, Social Security numbers and account numbers. We have no reason to believe that anyone has

> accessed or misused your information, but out of an abundance of caution, we have implemented internal monitoring to protect your personal and health information from misuse due to this incident."

The Privacy Officer next informs the GC that there are 46 states, and the District of Columbia, Puerto Rico and the U.S. Virgin Islands, that have data breach notification laws, many with unique requirements. Nuances among the state statutes include that 35 jurisdictions require notification only if there is likely to be a resulting risk of harm, 13 require notice to the applicable attorney general or other state agency, some have specific language to be included in the notification letter, many have requirements about timing of the notice and/or notification to law enforcement before notification to residents, and a handful of states apply their law to both paper and electronic records. Also, depending on the nature of the information and your field, federal laws may apply (although there is no uniform/mandatory federal breach notification law that applies to 1836 Technologies as opposed to the agencies themselves). She also goes on to inform you that under the EU Privacy Directive that there are national laws in Europe that also affect how and what information is protected and whether the company must notify the local Privacy Offices in each country. She understands but is not sure there are similar laws in India, Canada, and Australia.

Samantha Houston, the Information Assurance Officer is up next. She informs the GC that the company is supposed to have a first response team in place that includes persons in information technology, information security, compliance, business heads, human resources, legal counsel and public relations/investor relations. Unfortunately, the company had not yet stood up this team, and she is trying to implement the team on the fly. The GC asks her to assign tasks to team members and establish a point person, identify key personnel for each task, calculate timelines and set deadlines, communicate with management and establish attorney-client privilege for investigation and communications. The GC wonders how the government will react to this piece of information.

Finally, the GC calls in Jim Bowie, the now red-faced Compliance officer, who had not yet completed any of the policies that were supposed to be under review and/or implemented. She acknowledges that corporate rules for rigorous control of passwords had not been implemented, or that any training programs had been implemented at 1836 Technologies. He acknowledges that use of uncontrolled USB sticks, 3rd party accessing the company's network, and personnel utilizing unprotected wi-fi spots had been known but not counseled. He also acknowledges that it appeared that IT had been globally gathering data about individuals without their knowledge or permission. E-mail backup tapes and databases of personal information even remotely connected to the Internet had not been properly secured against compromise. The one saving grace is that all lap top computers had been encrypted, so that any information on the laptop, if stolen/lost would be unintelligible – of course if the ex-employee was the culprit, that would be of little solace to the GC or the Company, who decides that he has had enough for one day, and decides to call it a day and go down to the ACC reception and network with his brethren.

Extras from ACC

We are providing you with an index of all our InfoPAKs, Leading Practices Profiles, QuickCounsels and Top Tens, by substantive areas. We have also indexed for you those resources that are applicable to Canada and Europe.

Click on the link to index above or visit http://www.acc.com/annualmeetingextras.

The resources listed are just the tip of the iceberg! We have many more, including ACC Docket articles, sample forms and policies, and webcasts at http://www.acc.com/LegalResources.