# Partnering for Protection: Engaging with Your Info Security Team

Heidi Salow, Partner, Potomac Law Group PLLC

Christina Ayiotis, CRM, CIPP/E, AIGP, Assistant General Counsel, Lumen Technologies

# Disclaimer

*The information contained in this presentation both written and spoken is provided for informational purposes only and should not be construed as legal or business advice on any subject matter. No recipient of content, client or otherwise, should act or refrain from acting on the basis of any content included in the presentation without seeking the appropriate legal or other professional advice on the particular facts and circumstances at issue from an attorney licensed in the recipient's state. The presentation contains general information and may not reflect current legal developments, verdicts, or settlements. Potomac Law expressly disclaims all liability in respect to actions taken or not taken based on any or all of the content of this presentation.*

*The speakers provide this presentation (and written materials) solely in their personal capacity. Any and all opinions they express are theirs alone and do not represent the opinion(s) of any entities that employ them nor for which they do volunteer work.*

# HEIDI SALOW

Heidi has over two decades of experience advising entities of all sizes, including start-ups, Fortune 500 companies and non-profit organizations. She specializes in matters involving cybersecurity, data governance, data ethics, data privacy and data protection, employment-related privacy, healthcare privacy and security, insider threat management, mobile technologies, corporate risk management and social media. She has served as a strategic advisor to entities seeking to develop and implement legally compliant U.S. and global data protection programs in the information technology, media, telecommunications, retail, financial, healthcare and legal services industries.

## EDUCATION

- George Washington University, LL.M Program (all but thesis), Intellectual Property
- University of Baltimore, J.D.
- McGill University, B.A.

## PRIOR ROLES

- Leidos, Chief Privacy Officer
- Thomson Reuters, Vice President & Senior Privacy Officer
- Greenberg Traurig, Shareholder
- DLA Piper, Of Counsel
- Sprint Nextel Corp., Senior Counsel & Director

## REPRESENTATIVE EXPERIENCE AND CAPABILITIES

- Virtual/fractional Chief Privacy Officer (CPO) services
- Established the first Global Privacy Office function for a $13.5B global corporation
- Served as HIPAA Officer for $12.5B multi-national corporation with offices in 94 countries
- Counseled clients in the aftermath of 75-plus data breaches and data security incidents
- Created wide-reaching strategic plan for implementing Privacy by Design at a large corporation with multiple lines of business
- Developed and launched several new types of assessments, including HIPAA Risk Assessments, Privacy Threshold Assessments and Global Data Protection Assessments
- Negotiated 50-plus data processing, data sharing, data transfer, software licensing and HIPAA Business Associate Agreements
- Advised corporate security team on designing legally compliant insider risk management program
- Helped implement global data protection program for a multinational conglomerate with internal entities in the EU, U.S., Australia, Canada, Asia, Australia, and LatAm
- Advised Information Security Risk Management (ISRM) teams on Data Loss Prevention (DLP) governance programs
- Created employee training on a variety of privacy and cybersecurity topics, including HIPAA

# CHRISTINA AYIOTIS

Tina has over three decades of experience working both within the business, as well as providing legal services. She specializes in matters involving Cyber, Security, Privacy, Emerging Technologies, Artificial Intelligence, Litigation, Risk, Compliance, E-Discovery, and Knowledge Management. Her travel to 30 countries gives her the global context to strategize and create integrated, holistic, international solutions. In addition to being a Certified Records Manager and Certified Information Privacy Professional/Europe, she recently became certified as an Artificial Intelligence Governance Professional.

## EDUCATION

- William & Mary Law, J.D.
- Virginia Commonwealth University, B.S./B.A

## PRIOR ROLES

- OCC, Vice President, Security Services
- WiseLaw, Chief Cybersecurity Officer
- Georgetown Law Cybersecurity Law Institute, Founder/Co-Chair
- The George Washington University, Professorial Lecturer
- CSC, Deputy General Counsel
- Booz Allen, Corporate Records Manager
- Deloitte , GFSI Director
- Ernst & Young International, Regional (EMEA) Knowledge Account Manager

## REPRESENTATIVE EXPERIENCE AND CAPABILITIES

- As a SuperConnector, works cross-functionally/internationally to ensure greatest diversity of experience/thought
- Servant Leader/Continuous Learner/Legal Ambassador/Business Enabler/Early Adopter
- Within a regulated entity in financial services, improved compliance by creating a culture of privacy and security through policy, training, and leading by example
- Incorporated information governance (privacy, security, RIM, etc.) into organizational digital transformation
- Served on leadership team of a startup cyber law firm (in Australia on a Specialty Work Visa)
- Founded/Co-Chaired Georgetown Law Cybersecurity Law Institute (first such entity to approach cyber as both a Board-level business risk issue as well as a global national security threat/opportunity)
- As direct-report Deputy General Counsel to GC of a multinational (92,000 people in 80 countries), created first ever privacy- and security-compliant global E-discovery program; stood up new Global Privacy function
- Taught *Information Policy* course (for 7 years) in The George Washington University Department of Computer Sciences' Joint Master of Science- Graduate Certificate in Computer Security and Information Assurance Program
- Served on AFCEA International's Cyber Committee for 4 years (creating, *inter alia*, first legal panel at Annual Cyber Conference, as well as contributing to White Papers on Internet Governance and Government Cyber Strategy)

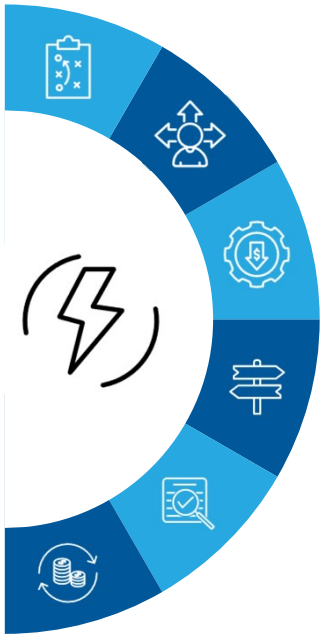


LUMEN®

# Agenda

- **The "What"**
    1. NIST Cybersecurity Framework 2.0
    2. Other Information Security Frameworks/Standards/Regulations (Examples)
    3. NIST Privacy Framework
    4. Privacy Overlay to ISO 27001 Security Standard: ISO/IEC 27701
    5. NIST AI Risk Management Framework
    6. NIST AI 600-1 Artificial Intelligence Risk Management Framework: Generative AI Profile
    7. Other AI Frameworks/ Standards/ Regulations
- **The "How"**
- **Key Actionable Steps You Can Take**

# NIST Cybersecurity Framework 2.0 (February 2024)



**Purpose**:

- Help organizations manage and reduce cybersecurity risks

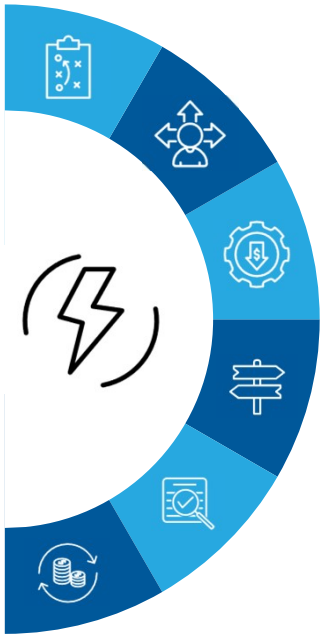
**Structure:**

- **Core Functions**: Govern, Identify, Protect, Detect, Respond, Recover
- **Profiles:** Tailored implementation of the core functions to specific organizational needs
- **Implementation Tiers:** Levels of cybersecurity risk management maturity

**Key Points:**

- Provides a taxonomy of high-level cybersecurity outcomes
- Flexible and adaptable to organizations of all sizes and sectors
- Links to additional resources for specific practices and controls

# A Few Other Information Security Frameworks/Standards/ Regulations



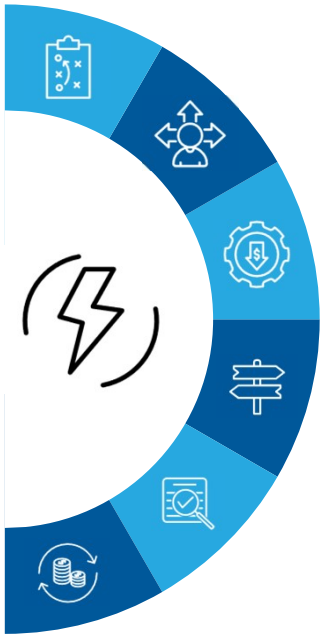
## Payment Card Industry Data Security Standard ("PCI DSS")

- Developed to encourage and enhance security for payment card data and facilitate the broad adoption of consistent data security measures globally
- Provides a baseline of technical and operational requirements designed to protect payment account data
- Deadline for implementing new v.4 requirements - March 31, 2025

## New York State Department of Financial Services Cybersecurity Regulation, 23 NYCRR Part 500

- Cybersecurity requirements for financial services companies
- First truly comprehensive cybersecurity law; served as a model worldwide because most of companies affected are global
- From investigating hundreds of cybersecurity incidents, NYDFS found there is a tremendous amount organizations can do to protect themselves - as a result, Part 500 was amended November 1, 2023

# A Few Other Information Security Frameworks/Standards/ Regulations (cont.)



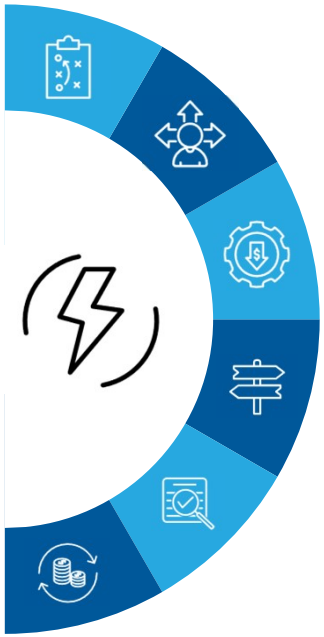
## ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

- World's best-known standard for Information Security Management Systems (ISMS)
- Defines requirements for an ISMS
- 2024 Amendment 1: Climate action changes

## ISO/IEC 27002: 2022 Information security, cybersecurity and privacy protection — Information security controls

- Provides guidance to establish, implement, and improve an ISMS focused on cybersecurity
- Offers best practices and control objectives related to key cybersecurity aspects including access control, cryptography, human resource security, and incident response
- Practical blueprint to effectively safeguard information assets against cyber threats
- Proactive approach to cybersecurity risk management and protect critical information from unauthorized access and loss

# NIST Privacy Framework



**Purpose**:

- Helps organizations manage privacy risks and protect individuals' privacy while fostering innovation

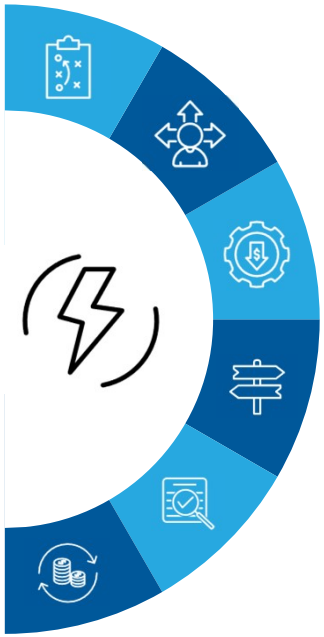
**Structure:**

- **Core Functions:** Identify, Govern, Control, Communicate, Protect
- **Profiles:** Tailored implementation of the core functions to specific organizational needs
- **Implementation Tiers:** Levels of privacy risk management maturity

**Key Points:**

- Voluntary tool for improving privacy through enterprise risk management
- Supports ethical decision-making and compliance with privacy regulations
- Flexible to address diverse privacy needs and technological trends

# Privacy Overlay to ISO 27001 Standard: ISO/IEC 27701



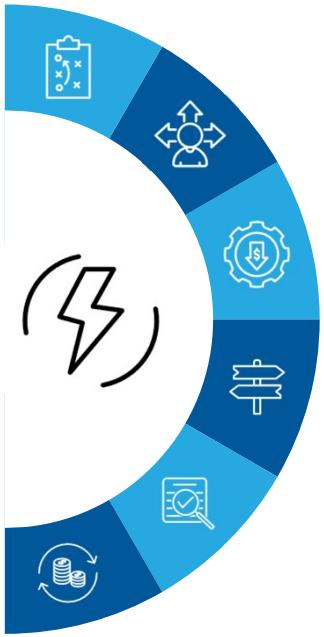
**ISO/IEC 27701: 2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management — Requirements and Guidance:**

- Guides organizations re: policies and procedures needed to comply with the EU GDPR and other data protection/privacy regulations and laws
- Specifies requirements for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS)
- Assists in the implementation of the controls
- Intended for Controllers and Processors of Personally Identifiable Information (PII)

**ISO/IEC DIS 27701.2 Information security, cybersecurity and privacy protection — Privacy Information Management Systems — Requirements and Guidance:**

- Draft document (most ISO standards are updated every 5 years)
- Under development

# NIST Artificial Intelligence (AI) Risk Management Framework



**Purpose**:

- Helps organizations manage risks associated with AI systems throughout their lifecycle

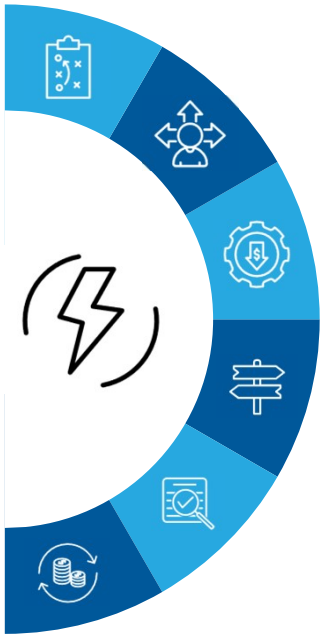
**Structure:**

- **Core Functions:** Govern, Map, Measure, Manage
- **Profiles:** Tailored implementation of the core functions to specific organizational needs

**Key Points:**

- Voluntary framework to support trustworthy and responsible AI
- Addresses risks such as bias, transparency, accountability, and security
- Developed through a collaborative, consensus-driven process

# NIST AI 600-1 Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (July 2024)



**Purpose**:

- Implementation of AI RMF for Generative AI ("GAI") – defines risks novel to, or exacerbated by, GAI

**Structure:**

- **Overview of 12 Risks Unique to or Exacerbated by GAI** (risks include **Data Privacy, Information Integrity, Information Security, Intellectual Property**)
- **Suggested Actions to Manage GAI Risks**

**Key Points:**

- This cross-sectoral profile is a companion resource to NIST AI RMF that can be used to help organizations govern, map, measure, and manage these risks
- GAI Risks vary along many dimensions such as **Stage of the AI Lifecycle, Scope, Source of Risk,** and/or **Time Scale**

# Other Artificial Intelligence (AI) Frameworks/Standards/Regulations

**MITRE ATLAS™ (Adversarial Threat Landscape for Artificial Intelligence Systems) is a Matrix for Security encompassing TACTICS, TECHNIQUES, and MITIGATIONS.**

- **Tactics**: the tactical adversary goals during an attack, are the "why" of a technique
- **Techniques**: the means to achieve tactical goals, are the "how" of the action
- **Mitigations**: represent the security concepts and classes of technologies to prevent a technique or sub-technique from being successfully executed

**MITRE ATLAS™ is a collaboration across industry, academia, and government and can be used to:**

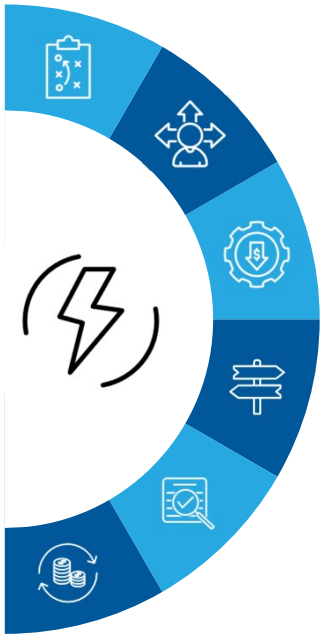
- Inform security analysts and AI developers/implementers of realistic threats to AI-enabled systems
- Enable threat assessments and internal red teaming
- Understand real-world adversary behaviors and mitigation pathways
- Report unique real-world adversary attacks on AI-enabled system

**NIST AI 100-2 E2023: Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations** (January 2024)

- " … taxonomy and terminology are meant to inform other standards and future practice guides for assessing and managing the security of AI systems, by establishing a common language and understanding of the rapidly developing AML landscape." https://csrc.nist.gov/pubs/ai/100/2/e2023/final

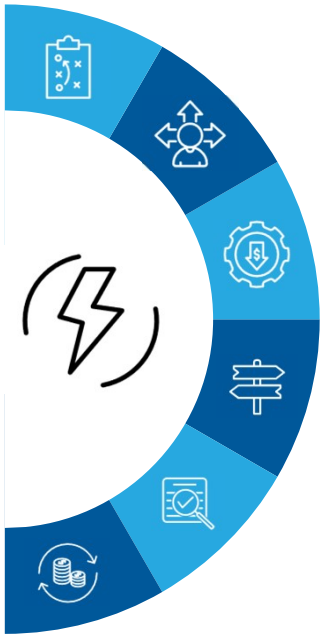
# Other Artificial Intelligence (AI) Frameworks/Standards/Regulations (cont.)

## U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency Artificial Intelligence (AI) Risk Categories and Mitigation Strategies for Critical Infrastructure



- Version 1.0; December 2023
- **Risk categories:**
  - Attacks Using AI (AI-Enabled Cyber Compromises; Automated Physical Attacks; Physical Target Identification; Social Engineering; Weapon Development)
  - Attacks on AI (Interruption of Service Attacks; Malicious Algorithmic Manipulation; Model Inversion and Extractions)
  - AI Design and Implementation Failures (Brittleness; Inscrutability; Overreliance on AI; Inadvertent Systemic and Design Flaws; Under Reliance on AI)

# Other Artificial Intelligence (AI) Frameworks/Standards/Regulations (cont.)



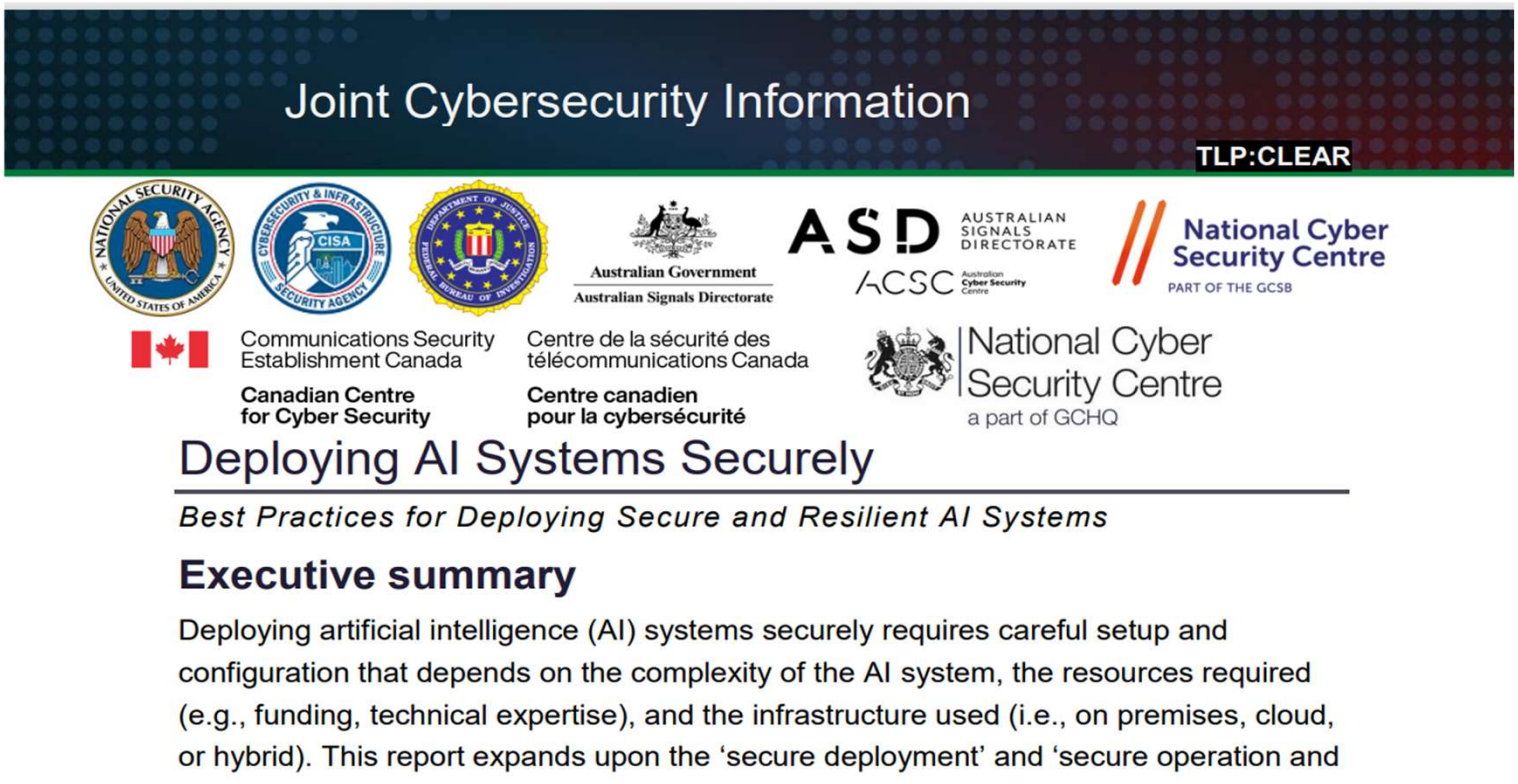
## U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency Artificial Intelligence (AI) Risk Categories and Mitigation Strategies for Critical Infrastructure (cont.)

**Select Mitigation Strategies:**

- Critical Data Inventory
- Cyber Incident Response
- Employee Vetting
- Information and Communication Technology (ICT) Supply Chain Risk Management
- Information Sharing Between Public and Private Sector
- Red Teaming
- Secure By Default/Design
- Software Bill of Materials
- User Security Awareness

# Other Artificial Intelligence (AI) Frameworks/Standards/Regulations (cont.)

**U.S. Department of Defense National Security Agency Joint Cybersecurity Information: Deploying AI Systems Securely: Best Practices for Deploying Secure and Resilient AI Systems (April 2024)**



Joint Cybersecurity Information

TLP:CLEAR

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

National Cyber Security Centre
PART OF THE GCSB

Communications Security Establishment Canada
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

## Deploying AI Systems Securely

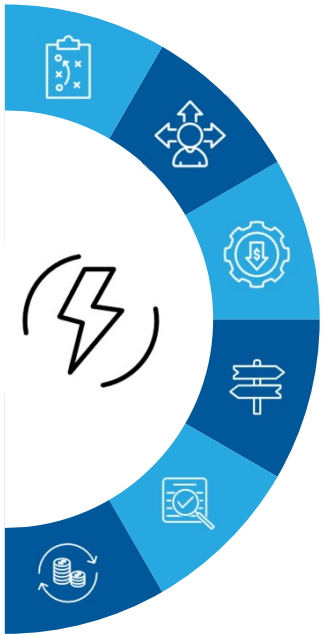
*Best Practices for Deploying Secure and Resilient AI Systems*

### Executive summary

Deploying artificial intelligence (AI) systems securely requires careful setup and configuration that depends on the complexity of the AI system, the resources required (e.g., funding, technical expertise), and the infrastructure used (i.e., on premises, cloud, or hybrid). This report expands upon the 'secure deployment' and 'secure operation and

# How to Implement these Frameworks, Standards, Laws and Regulations?

**All organizations, regardless of size, are responsible for security of sensitive, confidential and regulated data (including but not limited to *proprietary and personal* data), no matter where it is stored.**



**Legal departments can help security teams meet the requirements of these frameworks, standards and/or regulations by, for example:**

- Developing or updating policies and procedures, legal guidance, contracts (including contracts with service providers that handle sensitive, confidential and regulated data), and Incident Response Plans (IRPs)
- Meeting regularly with other stakeholders (e.g., Information Security, Information Technology, Human Resources, Corporate Communications teams) to collaborate and learn from each other
    - Consider co-chairing an Information Governance steering council or committee
- Hiring outside counsel to help with preparing this documentation – can provide specialized expertise and help with overflow work. Depending on circumstances and nature of the document, might also be protected by the Attorney Client Privilege

# Legal Departments Should Focus On:

**People, Process, Technology/ Platform**

**Holistic Approach**

**Promote Culture of Security**

# Legal Departments Should Focus On (cont.):

**Being a Proactive Business Partner/ Convener**

**Third Party Cyber Risk**

**Security by Design**

# Key Actionable Steps You Can Take

## If you work for a large company or organization:

- Set up meetings with your counterparts who are responsible for securing organizational systems and data (Corporate Security, Information Technology, Information Security) to determine how you can help them with their top priorities
  - these priorities likely go beyond just responding to incidents after they happen
- Address 3rd Party cyber and data security-related risks by a) reviewing vetting and onboarding processes for service providers/vendors, b) reviewing and continuously improving contracting processes, c) negotiating agreements with service providers/vendors which will handle any data deemed confidential, proprietary or sensitive
- Incorporate AI governance framework into the overall Enterprise Risk Framework (which should already include Cybersecurity and Privacy components)

## If you work for a small/smaller company or organization:

- For smaller organizations with limited resources, some functions will necessarily be outsourced
  - initial focus should be on front-end due diligence, contract language review, and audit assistance
- Identify and collaborate with key stakeholders in your organization, some of whom might have “dual” roles
- Incorporate AI Governance Framework into an overall Enterprise Risk Framework (which should already include Cybersecurity and Privacy components)

# Key Actionable Steps You Can Take (cont).

## Be an Engaged Advocate

- Support your colleagues and their mandate
- Enable security program implementation and continuous improvement to it
- Ensure role-based security training is created and effectively deployed
- Provide legal review and encourage business review of all security documentation (policies, standards, procedures, etc.)
- Stay abreast of regulatory/legislative developments and educate your counterparts on security teams so they can quickly and efficiently operationalize compliance

*All companies and organizations, regardless of size, should consider engaging outside subject matter experts and/or virtual/fractional CISO and CPO support*

# Thank you!

Heidi Salow, Potomac Law
hsalow@potomaclaw.com

Christina Ayiotis, Lumen Technologies
christina.ayiotis@lumen.com

## Questions

# PLG at a Glance

## Firm

- Sophisticated attorneys in a low-overhead environment
- The Best Lawyers in America, 2024
- Chambers ranked, 2024

## Attorneys

- 150+ attorneys, drawn from top global firms, many with in-house experience
- Attorneys have an average of 17 years' experience

## Clients

- National and international client base of 3,500 public and private companies and institutions
- Currently serve 10 percent of the Fortune 100

# Deeper Dive: Cybersecurity Requirements for Government Contractors

## CMMC

- US Department of Defense Proposed Rule (August 15, 2024): "DoD is proposing to amend the Defense Federal Acquisition Regulation Supplement (DFARS) to incorporate contractual requirements related to the proposed Cybersecurity Maturity Model Certification 2.0 program rule, Cybersecurity Maturity Model Certification Program."
- NIST 800-171 Rev.3: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (May 2024)
- Impact on contracting process: "The Defense Logistics Agency is in the process of automating some of its contracting systems, including verifying a contractor's compliance with the National Institutes of Standards and Technology's Special Publication 800-171. This is a step in the direction of implementing the new CMMC proposed rule, released last month, which would incorporate CMMC requirements into contracts and solicitations once finalized." Daisy Thorton, DLA turns to automation for head-start on incorporating CMMC requirements in contracting (federalnewsnetwork.com)

# Deeper Dive: Addressing 3rd Party Cyber Risk– Shared Security Model

## Center for Internet Security

*Shared Responsibility for Cloud Security: What You Need to Know*


Sources:

1. Microsoft Azure, https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

2. Amazon Web Services, https://aws.amazon.com/compliance/shared-responsibility-model/

# Resources


1. Privacy Framework | NIST - National Institute of Standards and Technology
2. NIST Privacy Framework: A Tool for Improving Privacy through Enterprise ...
3. AI Risk Management Framework | NIST
4. Artificial Intelligence Risk Management Framework (AI RMF 1.0) - NIST
5. Cybersecurity Framework | NIST - National Institute of Standards and ...
6. The NIST Cybersecurity Framework (CSF) 2.0
7. The NIST Privacy Framework: Overview and the 5 Functions
8. NIST Privacy Framework: An Overview - NIST Computer Security Resource ...
9. NIST's AI Risk Management Framework Explained
10. Understanding the NIST AI RMF: What It Is and How to Put It Into ...
11. Five Takeaways from the NIST AI Risk Management Framework
12. NIST Cybersecurity Framework 2.0: Resource & Overview Guide
13. AI 100-2 E2023, Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations | CSRC (nist.gov)
14. Cybersecurity Framework v2.0 - CSF Tools
15. https://doi.org/10.6028/NIST.AI.100-1
16. MITRE ATLAS™ https://atlas.mitre.org/ https://atlas.mitre.org/pdf-files/MITRE_ATLAS_Fact_Sheet.pdf
17. Guidelines for secure AI system development (ncsc.gov.uk) https://www.ncsc.gov.uk/files/Guidelines-for-secure-AI-system-development.pdf (2023)

# Resources (cont.)


18. FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence | The White House https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/
19. Machine learning principles (ncsc.gov.uk) https://www.ncsc.gov.uk/files/NCSC-Machine-learning-principles.pdf (2024)
20. AI and cyber security: what you need to know - NCSC.GOV.UK https://www.ncsc.gov.uk/guidance/ai-and-cyber-security-what-you-need-to-know (2024)
21. Engaging with Artificial Intelligence | Cyber.gov.au https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/artificial-intelligence/engaging-with-artificial-intelligence (2024)
22. The Artificial Intelligence Glossary | Legaltech News (law.com) https://www.law.com/legaltechnews/2023/05/08/the-artificial-intelligence-glossary/ (last updated March 2024)
23. Key Terms for AI Governance (iapp.org) https://iapp.org/resources/article/key-terms-for-ai-governance/ (last updated July 2024)