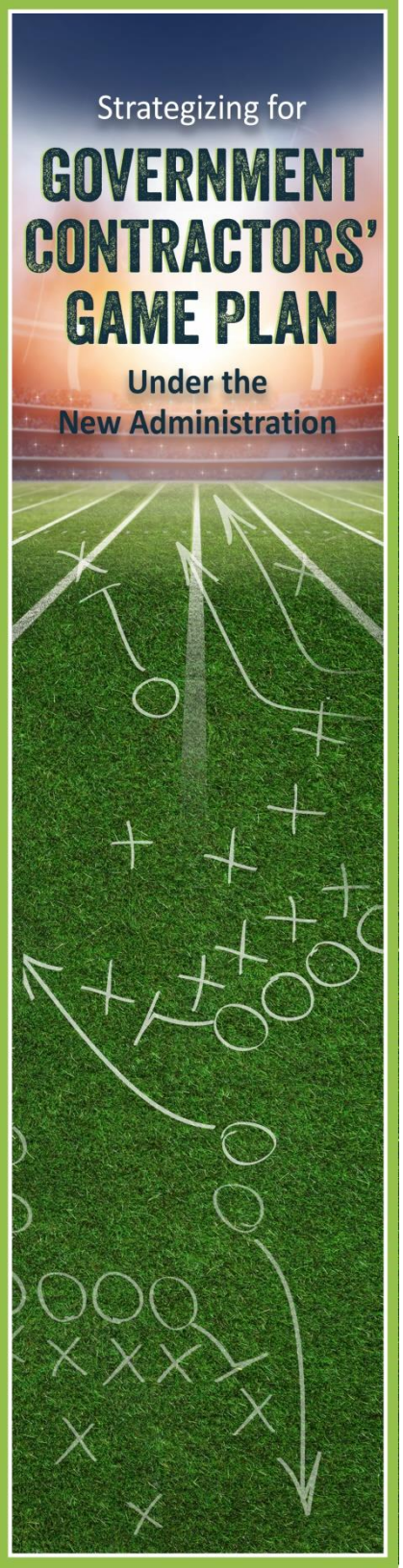

# Hurry-Up Offense: Keeping Pace with Information Security and Privacy

Peter Miller

Paul Rosen

Evan Wolff

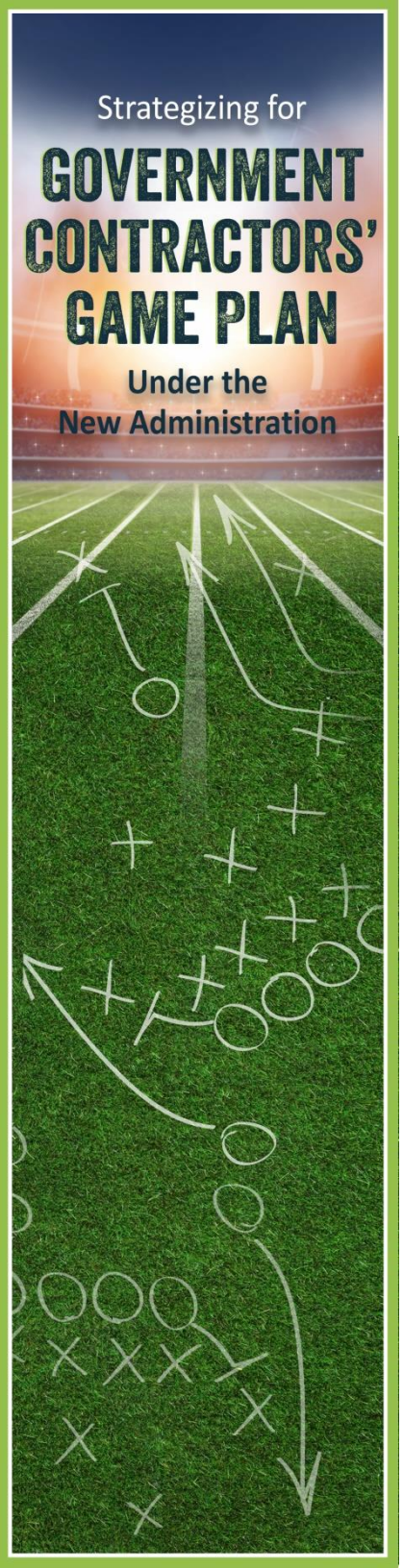
Kate Growley




crowell moring

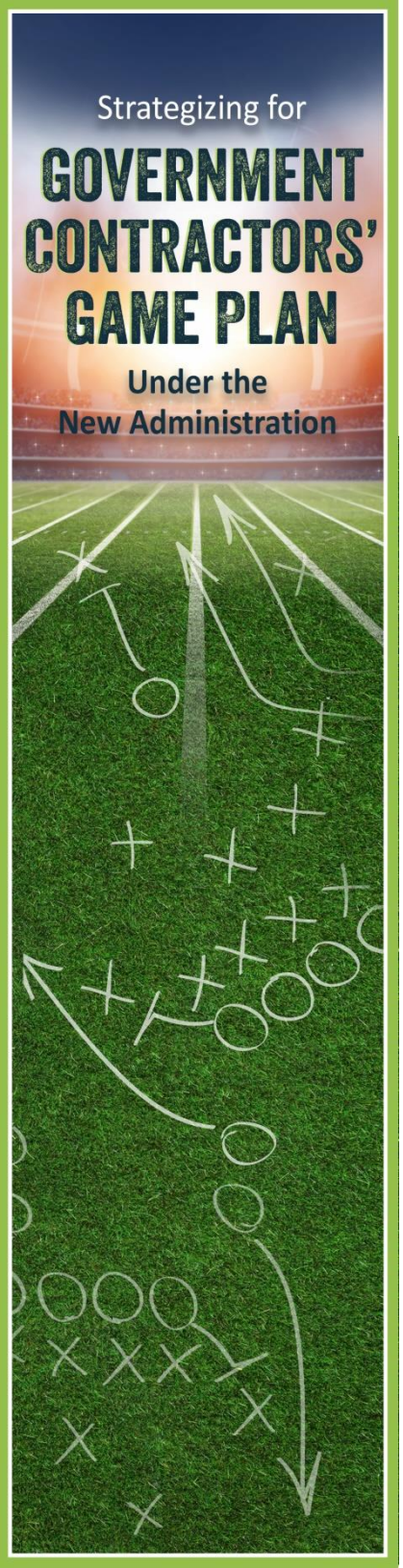
# Game Plan: Information Security & Privacy Risk

- Managing "Ordinary" Information Security & Privacy Risk
  - Legal Principles, Information Sharing, and Incident Preparation/Response
- Managing Government Contracts Information Security & Privacy Risk
  - Risk Environment, DFARS/FAR/NIST, Insider Threats, and Investigations
- Managing Business Life Cycle Information Security & Privacy Risk
  - Governance, Business Transitions, and Vendor Management




crowell moring

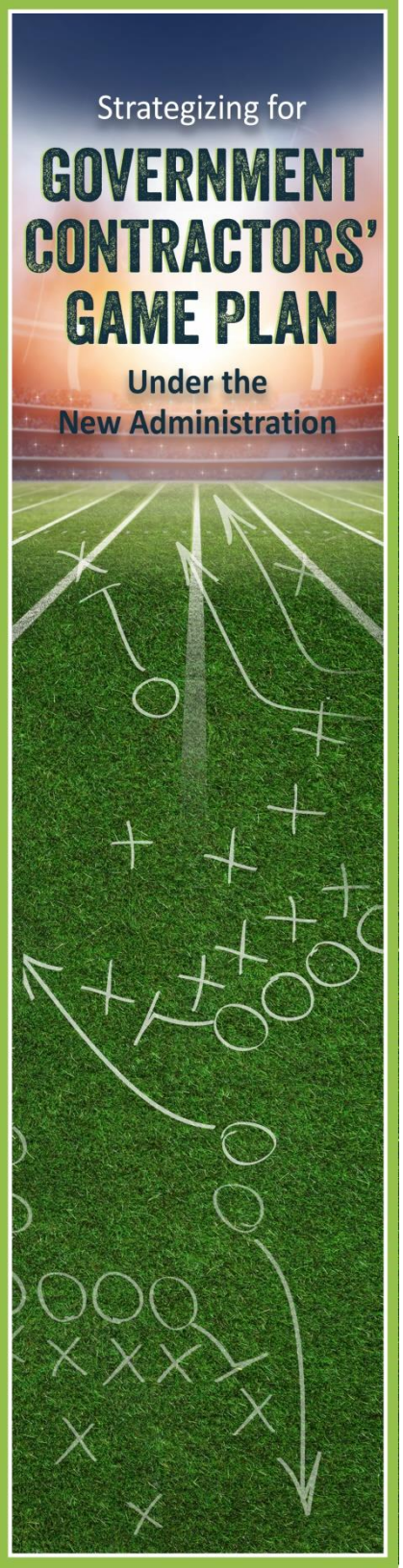
# Managing 'Ordinary' Information Security and Privacy Risk




crowell moring

# Privacy & Data Security Guidance

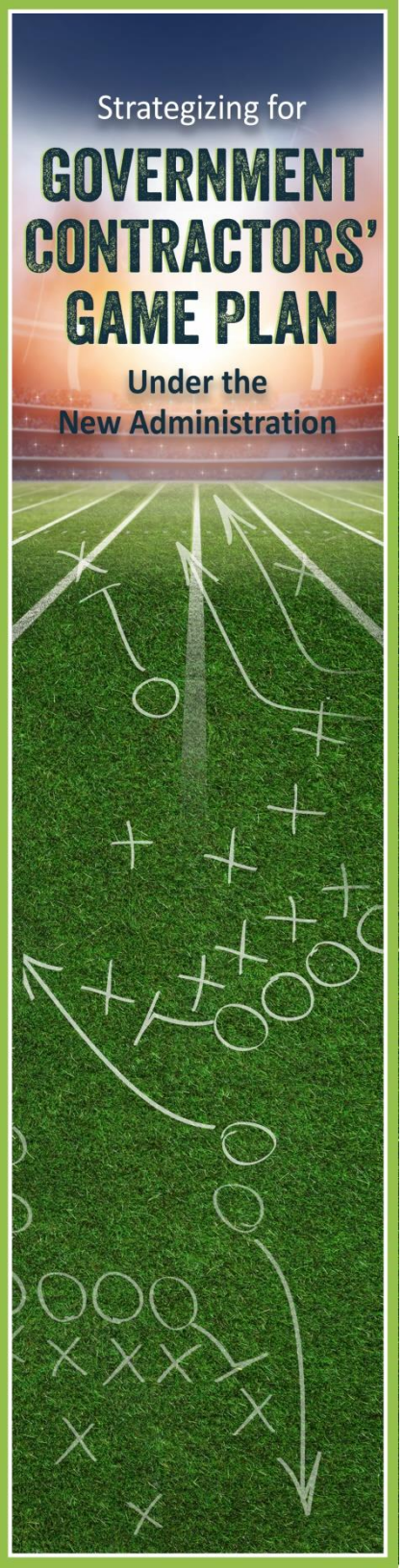
- Federal and State Law Patchwork
  - Privacy, data security, incident response
  - Multiple regulators (sectors, industries, conduct)
  - Private rights of action
- International Law
  - GDPR, APEC, regional and local laws, including data transfers, data localization,
- Contract-Specific Obligations
- Fair Information Practice Principles (FIPPs)
  - Privacy by Design
  - Security by Design
- Industry Best Practices
- Certification Programs
- Self-Regulation Programs




crowell moring

# Selected Data Types and Risk Considerations

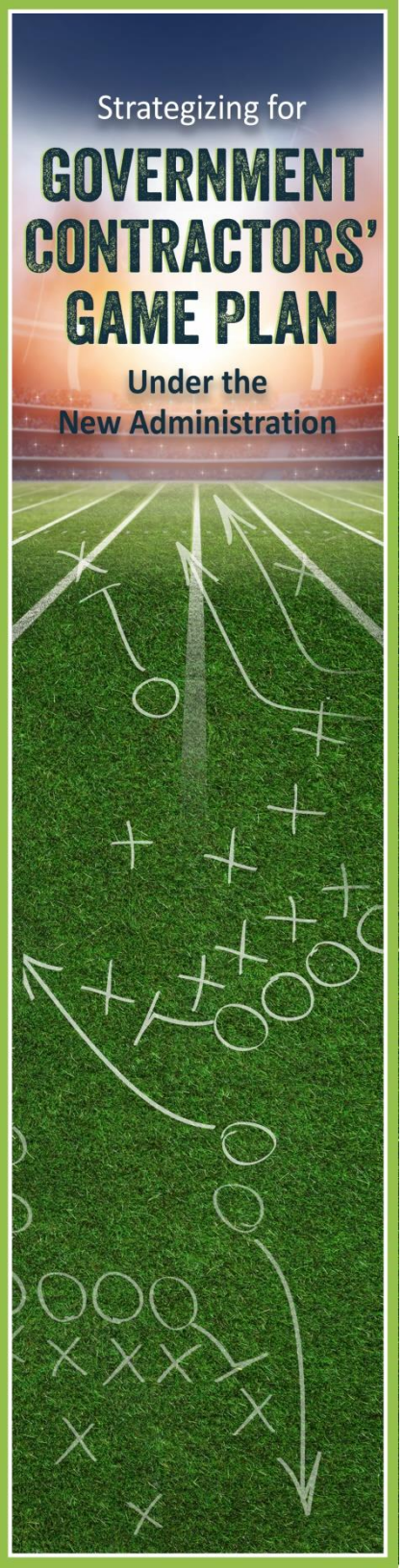
| DATA TYPE | COMPLIANCE & RISK CONSIDERATIONS |
|---|---|
| **Personal information (Personally Identifiable Information (PII))** | • Federal Law (e.g., Privacy Act, E-Government Act of 2002, FISMA; FTC Act), and sector-specific laws, below<br>• State privacy, security, and data breach notification laws<br>• International laws on collection, use, and transfer |
| **Protected Health Information (PHI)** | • Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act<br>• Federal and State laws regarding medical and health information<br>• International laws on collection, use, and transfer |




crowell moring

# Selected Data Types and Risk Considerations (cont.)

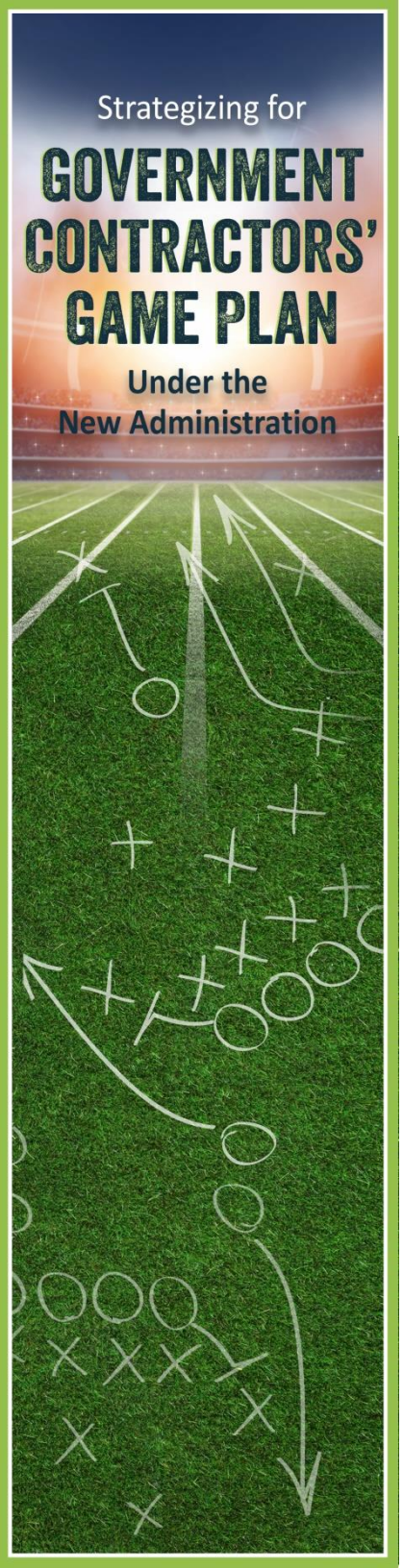
| DATA TYPE | COMPLIANCE AND RISK CONSIDERATIONS |
|---|---|
| **Intellectual Property/Proprietary Information** | • Copyright, trademark, patent, and trade secrets law and regulations<br>• Contractual obligations |
| **Government Information** | • Federal contract requirements (FAR and DFARS)<br>• National Industrial Security Program Operating Manual (NISPOM)<br>• NIST Cybersecurity Framework and Data Security Guidance<br>• State laws |




crowell moring

# Managing Risk with Effective Incident Response: Prepare, Practice, and Execute

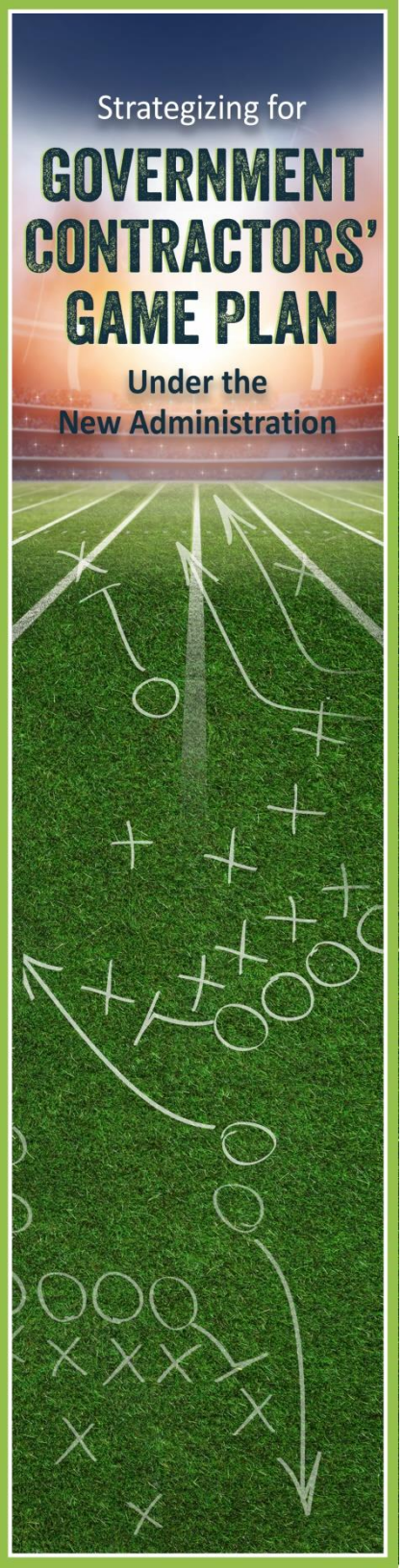
- Incident response plan
- Incident response team (IRT), including third parties (counsel and forensics)
- Regular tabletop exercises
- Investigation triggered by incident report -- Focus on security, mitigation and evidence gathering
- Manage external risks
  - Government (Federal and state)
  - Insurance
  - Communication
  - Individuals
  - Business partners and vendors
- Incident-related legal and contractual compliance
- Anticipate litigation




crowell moring

# Teamwork: Managing Risk with Information Sharing

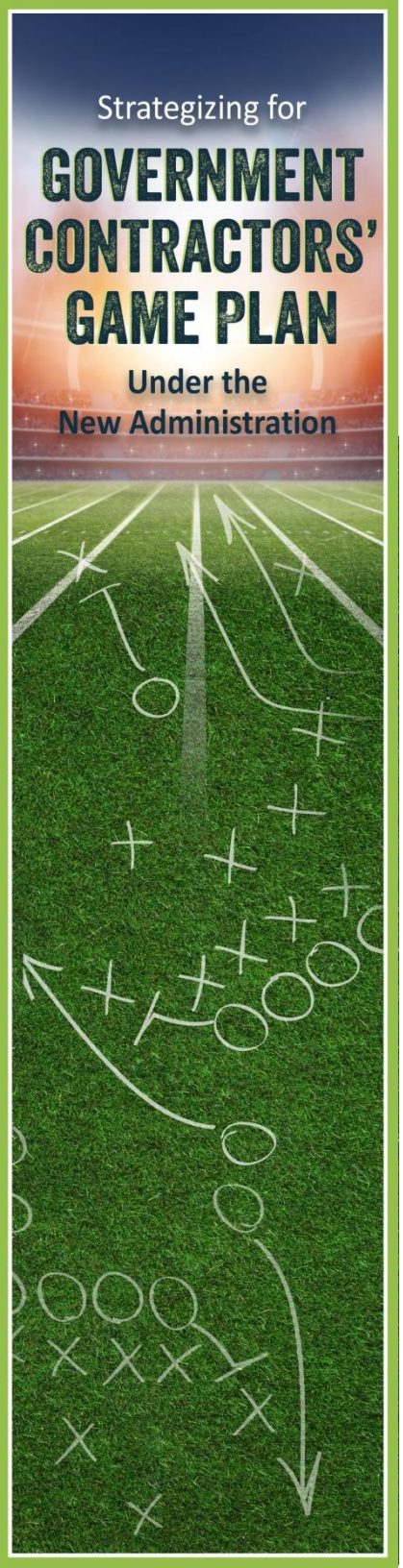
- E.O. 13691: Promoting Private Sector Cybersecurity Information Sharing
- DOJ/FTC Policy Statement "Sharing of Cybersecurity Information"
- Cybersecurity Information Sharing Act (CISA)
  - Any "non-federal entity" can share information with federal government "notwithstanding any other provision of law."
  - Information-sharing portals
  - Liability protections
- NIST Guide to Cyber Threat Information Sharing (NIST Special Publication 800-150, 10/16)




crowell moring

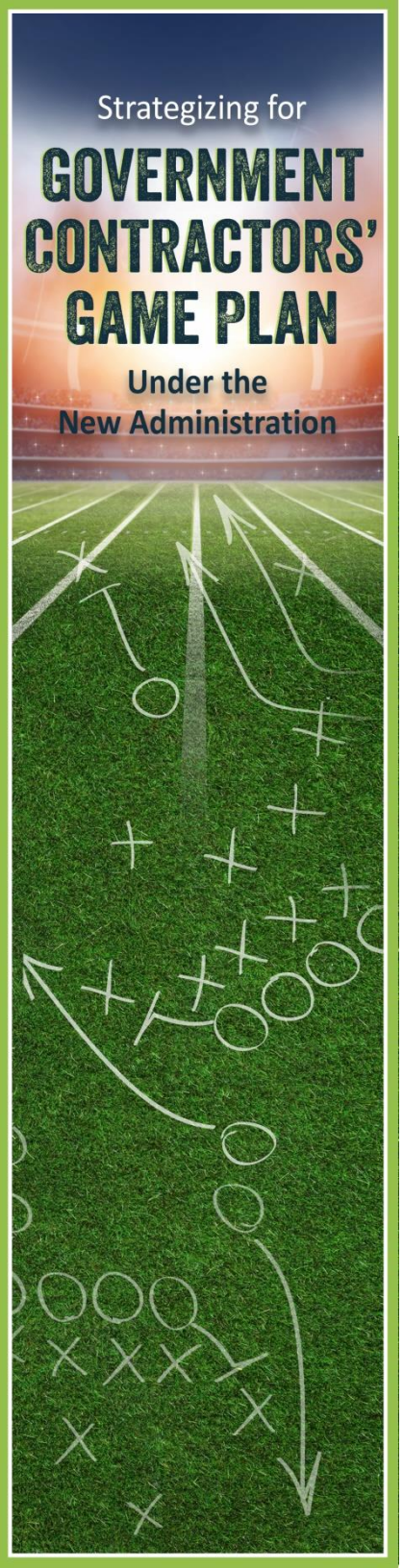
# Information Sharing Considerations

- Privacy and information security
- Antitrust
- Contract terms:  IP and vendor agreements
- Weighing benefits and risks
- Sector best practices




crowell moring

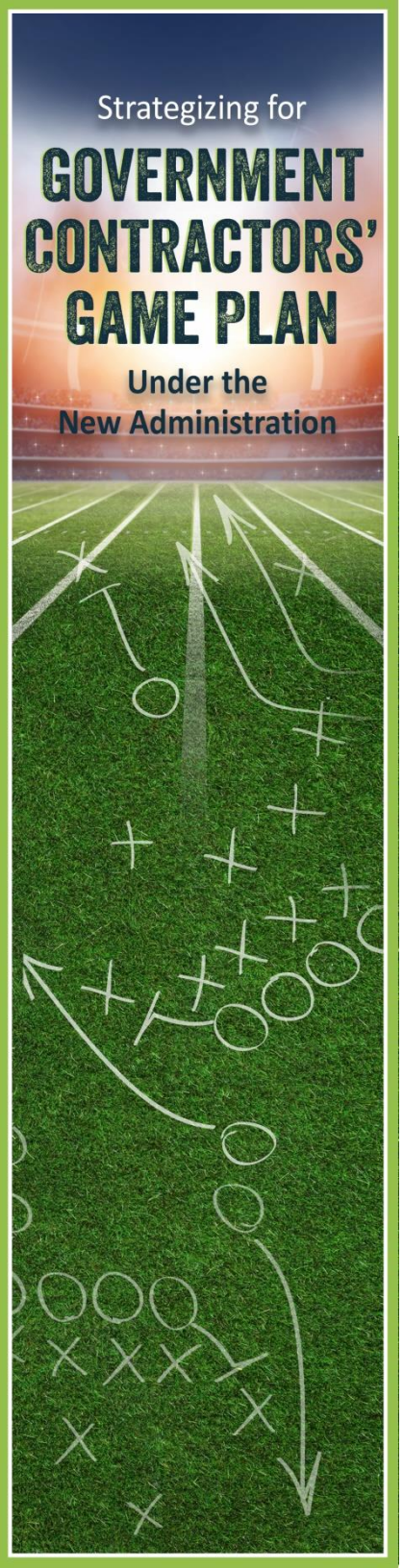
# Managing Government Contracts Information Security and Privacy Risk




crowell moring

# Current Threat Environment

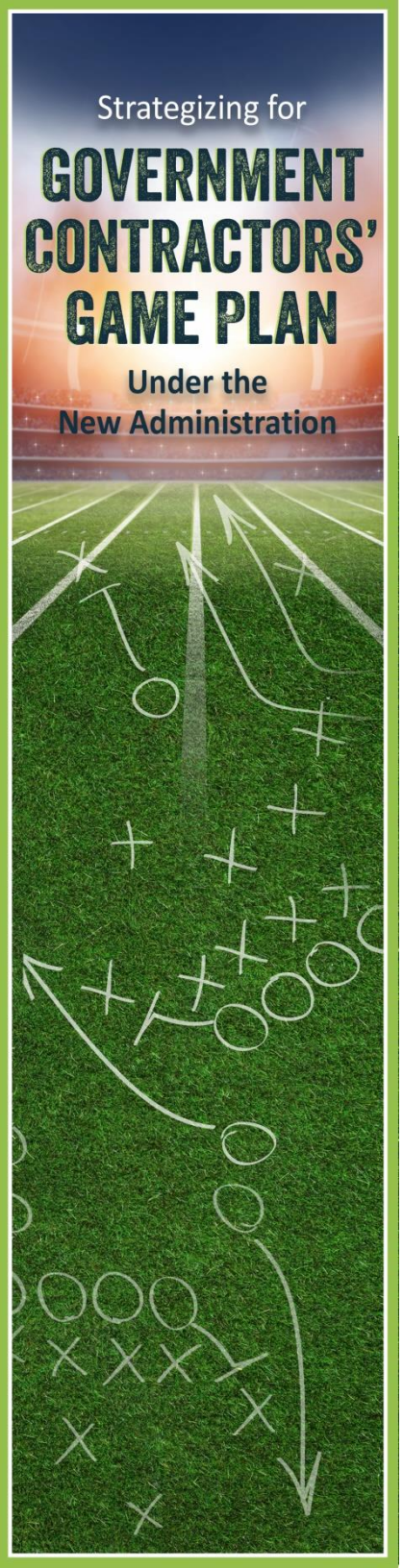
- Government Agencies, Systems, and Data
- Government Contractors, Vendors, and Subs
- Critical Infrastructure
- Private Sector




crowell moring

# New National Archives Controlled Unclassified Information (CUI) Program, 32 C.F.R. § 2002

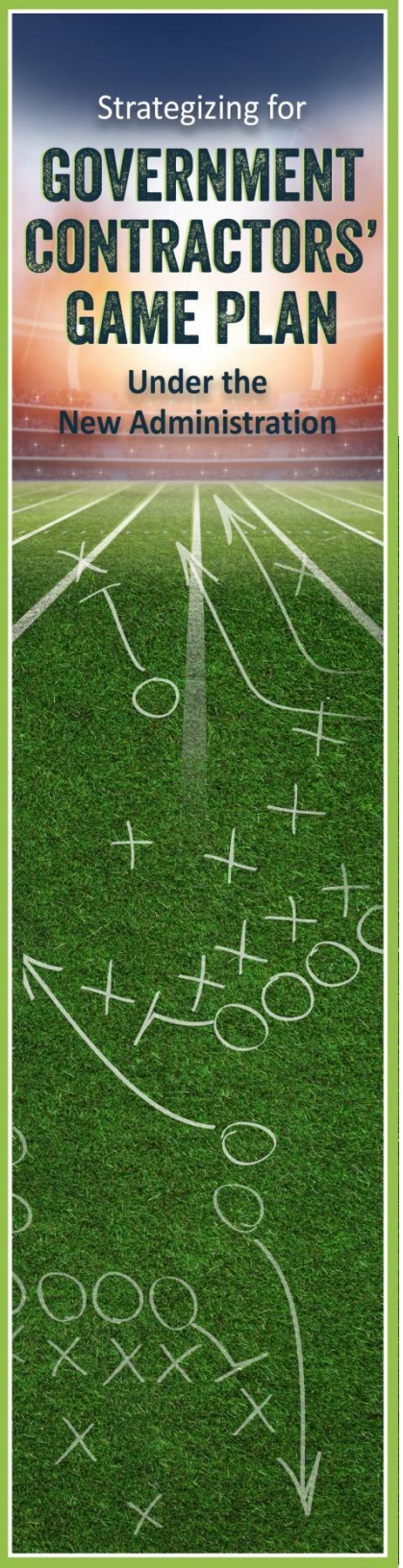
- Government-wide, consistent approach to identifying and handling sensitive information
- September 2016 final rule speaks to agency requirements
- Still waiting on corresponding FAR Clause for contractors
  - Requirements for marking, handling, and transmitting CUI
  - Imposing NIST SP 800-171
  - Reporting non-compliance




crowell moring

# Revised DFARS 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*

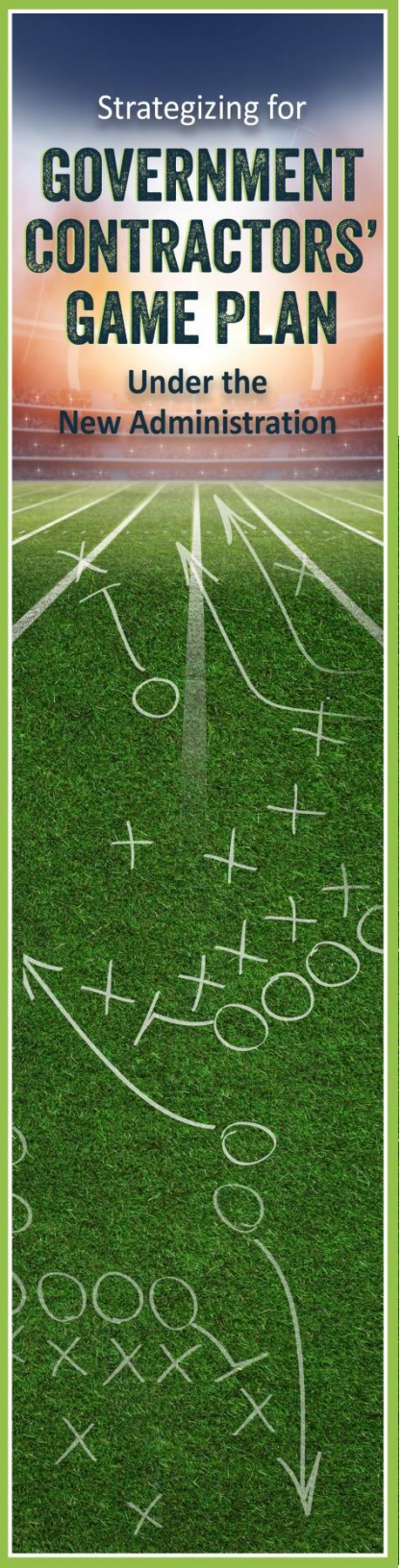
- Revised and final rule issued October 2016
  - CUI + DoD = Covered defense information
  - Requirements for external cloud services
  - Articulates sub notifications to primes
- NIST SP 800-171 Rev. 1 published December 2016
  - New control requiring system security plans
- Industry Information Day announced
  - June 23, 2017 in Alexandria, VA




crowell moring

# Federal Systems & Federal Information

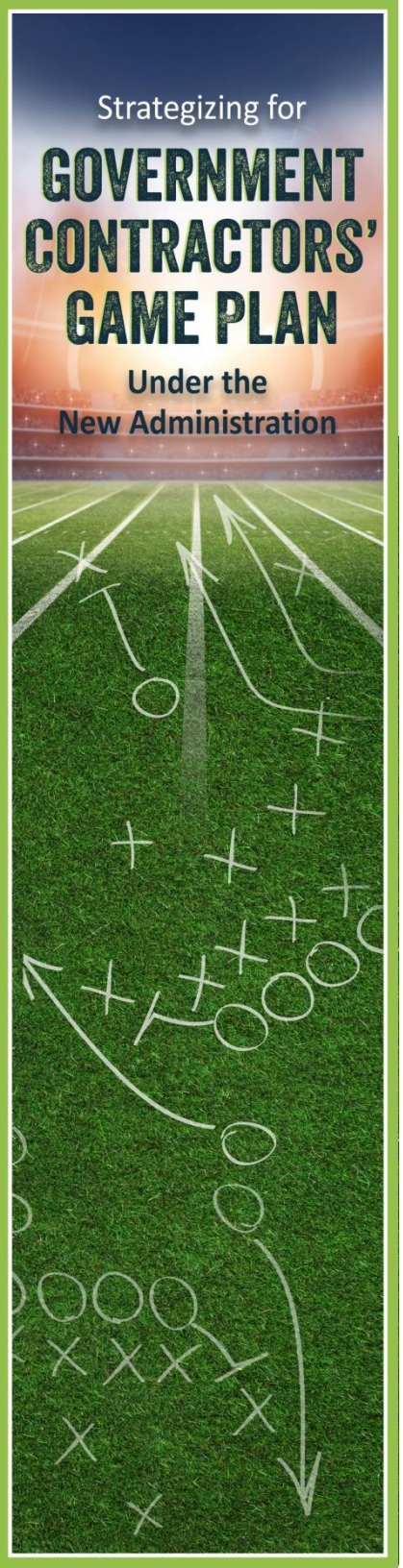
- FISMA (2014 revision)
  - Increased accountability, reporting and oversight for data security and privacy
- Revised OMB Circular A-130 (July 28, 2016)
  - Data security and privacy are "crucial elements of a comprehensive, strategic, and continuous risk-based program"
  - Agency contracts must "enable agencies to meet Federal and agency-specific requirements pertaining to the protection of Federal information"
- Privacy Training Requirement, FAR Subpart 24.3 (Dec. 20, 2016; eff. Jan. 19, 2017))
  - Applies to all who work with Privacy Act systems of records and federal PII, with flowdown requirement
  - Specified training requirements include Privacy Act, working with federal PII, incident response, and potential civil and criminal consequences for violations




crowell moring

# Tackling Insider Threats (Change 2 to DOD 5220.22-M (NISPOM)

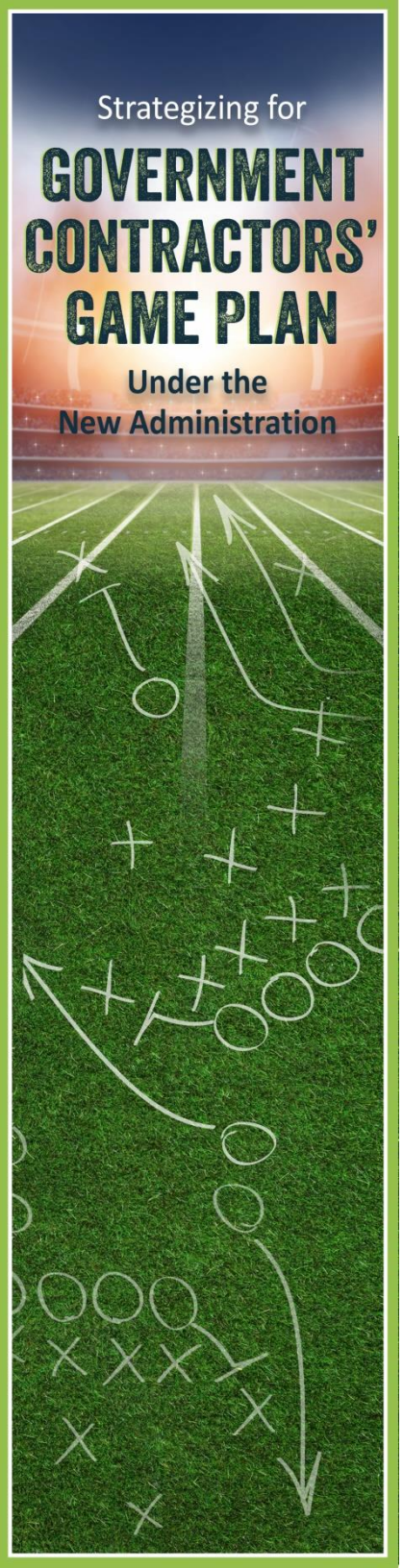
- Contractors with cleared facilities must "establish and maintain an insider threat program [ITP] that will gather, integrate, and report relevant and available information indicative of a potential or actual insider threat"
  - ITP scope: information covered by 13 personnel security adjudicative guidelines.
  - Annual self-inspection by ITPSO, report subject to DSS inspection
- "Insider threat" – Use of "authorized access, wittingly or unwittingly, to do harm to the national security of the United States," including "harm to contractor or program information" that impacts "obligations to protect classified national security information."




crowell moring

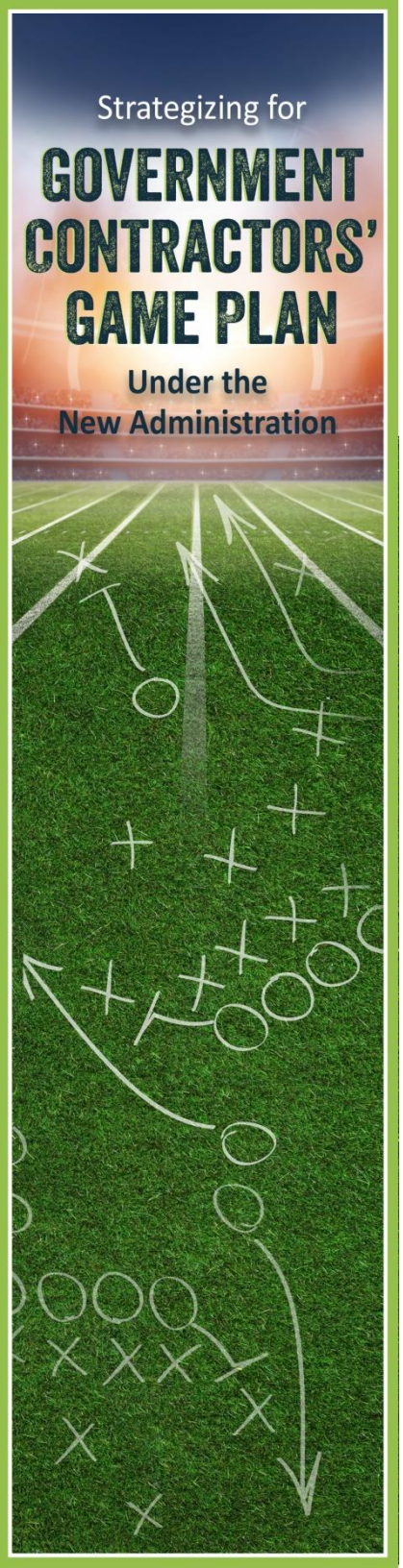
# Tackling Insider Threats (cont.)

- Training and awareness requirements (3-103)
  - Specific content requirements
  - Initial training prior to access, then annually
  - Training records subject to DSS review
- Information Security Controls (Chap. 8)
  - DSS-provided information system security controls, including monitoring notice
  - Controls based on FISMA and NIST
- ITP implementation tips
  - Create an interdisciplinary ITP team (HR, OGC, IT, and operational components)
  - Review policies and procedures, particularly with regard to information security and privacy
  - Tailor ITP resources to organization's size, activities, and risks




crowell moring

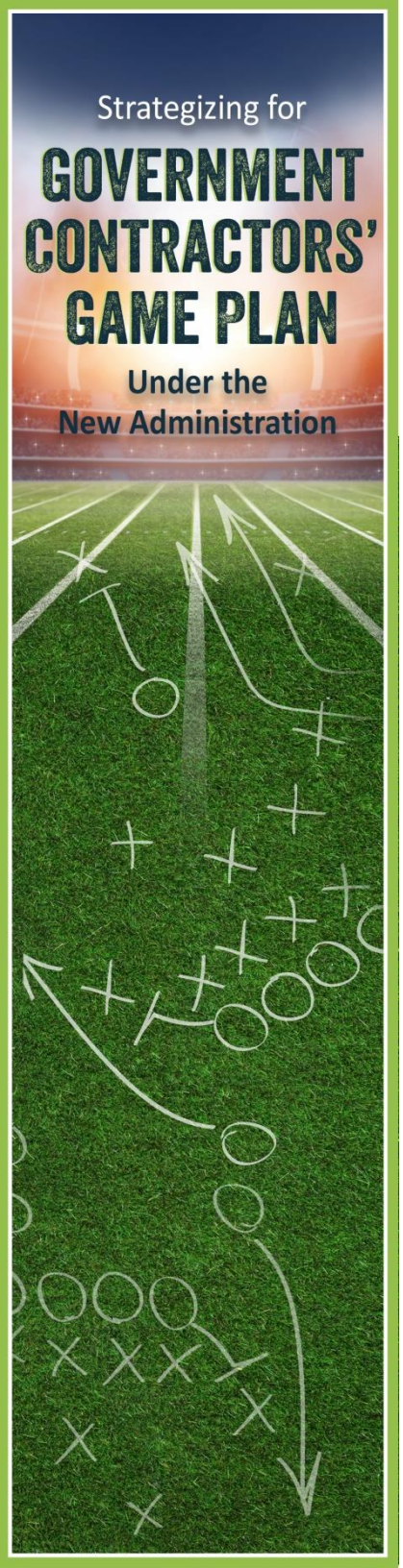
# Managing Information Security and Privacy Risk During the Business Lifecycle




crowell moring

# Managing Ordinary and Government Contract Risk Throughout the Business Lifecycle

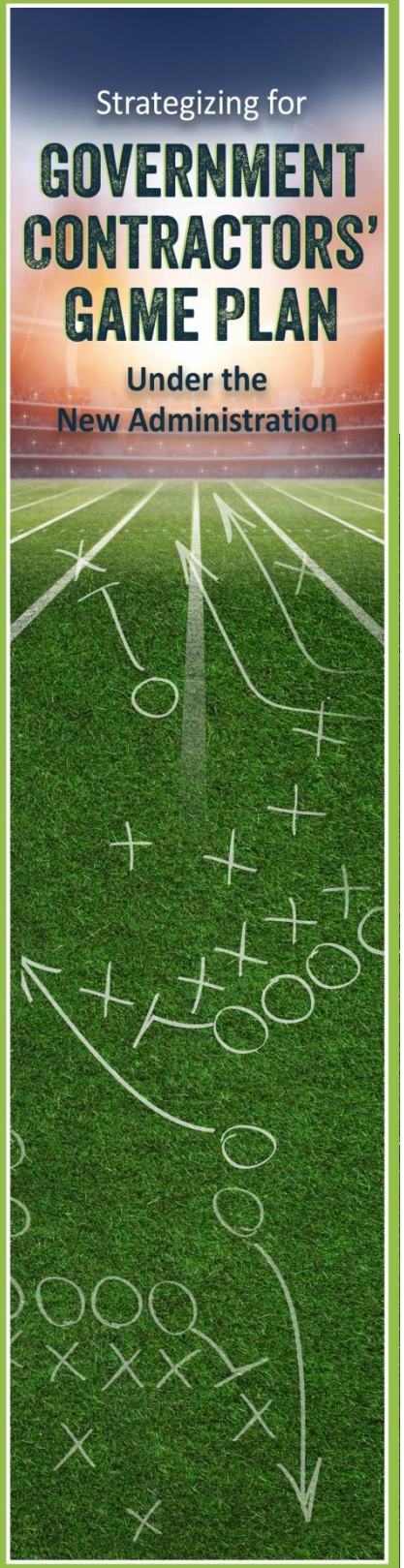
- Governance
- Corporate policies and procedures, especially Incident Response Plan
- Vendor management, compliance terms, and flowdown
- Business transactions and privacy and information security due diligence
- Training and awareness




crowell moring

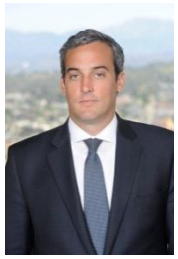
# Post-Game Wrap-Up: Managing Information Security & Privacy Risk

- Identify and Classify Data and Systems (CUI? Classified? PII? Regulated?)
- Implement Physical, Technical, and Administrative Controls to address risks, compliance and otherwise
- Establish Appropriate Governance
- Review and Update Policies & Procedures Regularly
- Evaluate Whether Public-Facing Statements on Security and Privacy Match Current Practices
- Prepare for Data Incidents in Advance (Incident Response Plan, Team, Tabletop, Data Breach Toolkit)
- Review Vendor Management Process
- Analyze Audit and Reporting Processes
- Conduct Training
- Participate in Industry and Government Partnerships




crowell moring

# Contacts / Questions



Paul Rosen
Partner
213-443-5577
prosen@crowell.com

Evan Wolff
Partner
202-624-2615
ewolff@crowell.com

Peter Miller
Senior Counsel
202-624-2506
pmiller@crowell.com

Kate Growley
Counsel
202-624-2698
kgrowley@crowell.com