Recent Data Security Developments for Government Contractors

November 4, 2015

WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Attorney Advertising

Speakers

Jonathan Cedarbaum
Partner
WilmerHale

Barry Hurewitz
Partner
WilmerHale

Ben Powell
Partner
WilmerHale

Jason Chipman
Counsel
WilmerHale

Leah Schloss
Associate
WilmerHale

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A box on the bottom right panel
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*
- WebEx customer support: +1 888 447 1119, press 2

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Please note that no partial credit will be awarded. Attendees requesting CLE credit must attend the entire program.

Agenda

I. Introduction: Framing Cybersecurity for Contractors

II. Overview of Legal Landscape

III. Recent Developments

- A. FISMA/OMB Guidance
- B. Interim DFARS Rule on Network Penetration Reporting/Cloud Computing

IV. Breach Preparedness and Response

Government Continues to be a Key Target

OPM Breach is Just the Latest

Contractors are Key Proxy Target for Government

abc NEWS

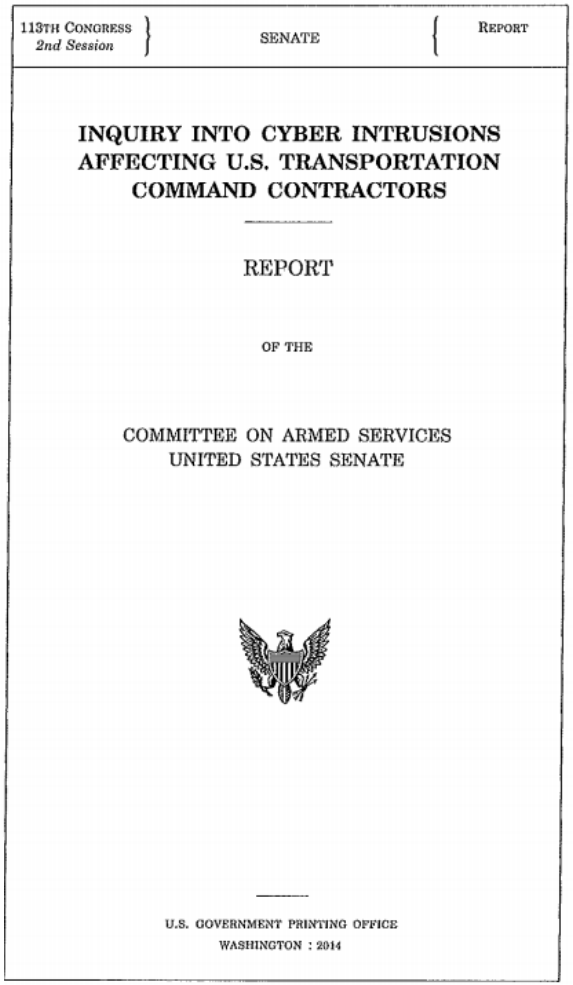
Feds Eye Link to Private Contractor in Massive Government Hack

REUTERS

Chinese hacked U.S. military contractors: Senate panel

The Washington Post

DHS contractor suffers major computer breach, officials say



113TH CONGRESS *2nd Session* } SENATE { REPORT

INQUIRY INTO CYBER INTRUSIONS AFFECTING U.S. TRANSPORTATION COMMAND CONTRACTORS

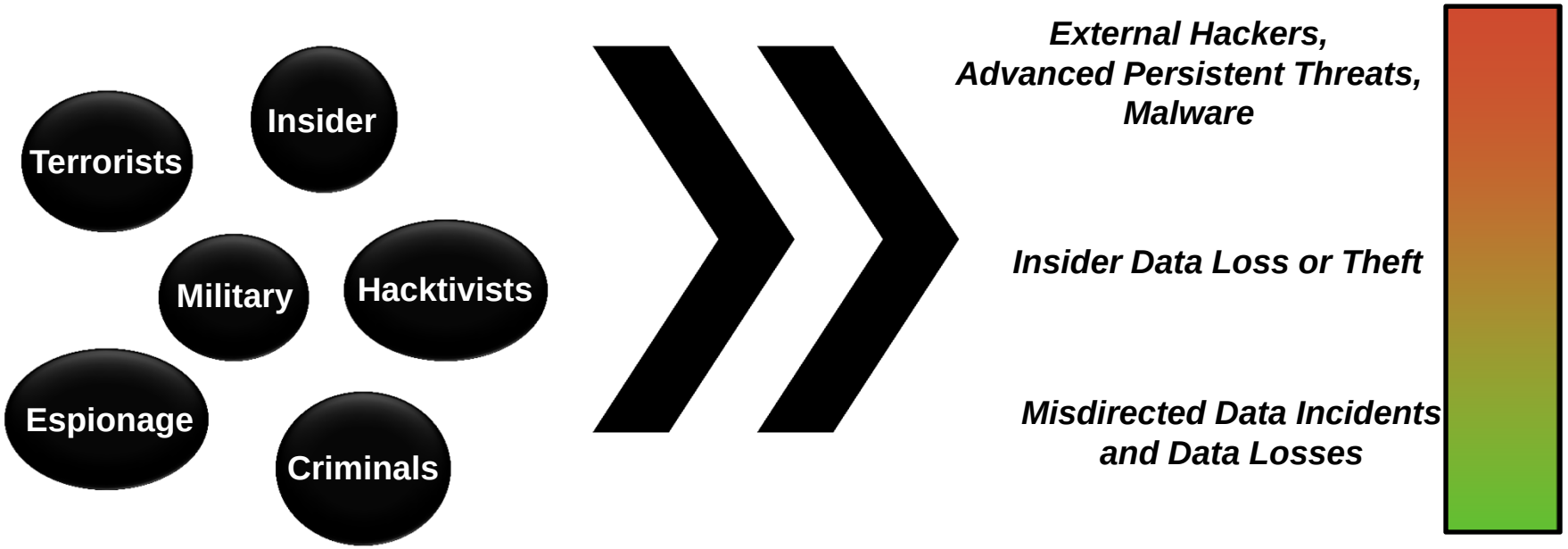
REPORT

OF THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2014

Variety of Attackers and Modalities



Overview of Legal Landscape

A. Federal Information Security Management Act ("FISMA")

B. Other Sources

   i. FAR/DFARS/Other FAR Agency Supplements (or special contract clauses)

   ii. Privacy Act

   iii. Federal Risk and Authorization Management Program ("FedRAMP")

C. Executive Order 13636

Federal Information Security Management Act ("FISMA")

- Purposes:
  - Provide a comprehensive framework for ensuring effectiveness of information security controls;
  - Establish government-wide management and oversight of federal information security risks; and
  - Set minimum controls to protect Federal information and information systems.
- Authorized OMB to oversee agency information security policies and practices.
- Required each agency to develop information security protections, and conduct annual evaluation for report to OMB.

FISMA (continued…)

- Agencies responsible for protection of "information systems used or operated . . . by a contractor of an agency or other organization on behalf of an agency" → Flows down to contractors.
- Federal Information Security Modernization Act of 2014
  - Authorizes DHS to assist OMB in administering implementation of agency information and security practices.
  - Modify scope of agency reporting requirements.
  - Within one year of enactment, OMB required to revise Circular A-130 (last updated in 2000) to eliminate inefficient or wasteful reporting.

Other Sources

- FAR/DFARS/other FAR Agency Supplements (or special contract clauses)
  - DFARS Provision on Unclassified Controlled Technical Information ("UCTI")
  - Supply Chain Rule
- Privacy Act
- Federal Risk and Authorization Management Program ("FedRAMP")

Executive Order 13636

- Executive Order on Improving Critical Infrastructure Cybersecurity (February 2013)
  - Directed NIST to develop Cybersecurity Framework
  - Tasked agencies with harmonizing existing cybersecurity procurement requirements.
  - Directed GSA and DoD to prepare recommendations on the "feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration."

Executive Order 13636 (continued…)

- GSA-DoD Joint Working Group Report: *Improving Cybersecurity and Resilience Through Acquisition*
  1. Institute baseline cybersecurity requirements as condition for contract award;
  2. Train government workforce in cyber acquisition practices;
  3. Develop common definitions;
  4. Create Government-wide cyber risk management strategy to identify acquisitions with greatest cyber risk;
  5. Secure the supply chain through OEMs, authorized resellers, and other trusted sources; and
  6. Increase accountability among key decision-makers.

Recent Developments

A. FISMA/OMB Guidance

B. Interim DFARS Rule on Network Penetration Reporting/Cloud Computing

C. Current Status and Looking Forward

FISMA/OMB Guidance

- OMB Guidance on Improving Cybersecurity Protections in Federal Acquisitions
- Civilian Agency “Cyber Sprint”
- FY16 OMB FISMA Guidance
- Revision to OMB Circular A-130

OMB Guidance: Improving Cybersecurity in Federal Acquisitions

- **Security Controls.** Compliance with NIST Special Publications requiring access controls, training, auditing, configuration management, authentication, incident response, risk assessments, etc.
- **Cyber Incident Reporting.**
  - Applies to systems containing CUI or operated for government.
  - Ensure that all known or suspected incidents be reported to agency CSIRT/SOC within agreed-upon timelines.
  - Reported incident is not itself evidence of failure to provide adequate safeguards.

OMB Guidance (continued…)

- **Information System Security Assessments.** Use ATO or other independent assessments as indication of common controls and capabilities.
- **Information Security Continuous Monitoring.**
  - BPA for Continuous Diagnostics and Mitigation program.
  - Intended to ultimately integrate with EINSTEIN.
- **Business Due Diligence.**
  - GSA to create diligence shared service.
  - CIO/CAO Councils will make recommendations on risk indicators as baseline for diligence.

OMB Guidance (continued…)

- Criticism of OMB Guidance
  - No meaningful standardization.
    - General statements with explicit allowance for agencies to deviate.
    - Should provide for more harmonization between agencies, while allowing contractors greater flexibility with specific controls used.
  - No coordination with agency-specific actions.
    - Overlap
    - Inconsistencies
  - Significant gaps (e.g., lack of key definitions, industry outreach, etc.).

Civilian Agency “Cyber Sprint”

- 30-day “sprint” launched in June by Federal CIO after OPM breach.
- Last week, OMB issued memo summarizing sprint: Cybersecurity Strategy and Implementation Plan for Federal Civilian Government.

Civilian Agency "Cyber Sprint" (continued . . .)

CSIP Implementation – Key Milestones*

Milestones		Oct. 1, 2015 – Dec. 31, 2015	Jan. 1, 2016 – Mar. 31, 2016	Apr. 1, 2016 – June 30, 2016	July 1, 2016 – Sept. 30, 2016
Objective 1: Identify	DHS delivers full CDM Phase 2 capabilities to participating agencies				September 30, 2016
	All agencies identify and report High Value Assets	November 13, 2015			
Objective 1: Protect	OMB releases plan for implementing new cybersecurity shared services		January 31, 2016		
Objective 2: Detect	DHS makes EINSTEIN 3A protections available to agencies not covered by E3A providers	December 31, 2015			
Objective 2: Respond	OMB issues Federal incident response best practices	October 30, 2015			
	GSA delivers an incident response contract vehicle			April 30, 2016	
Objective 3: Recover	NIST issues guidance to agencies on recovering from cyber events				June 30, 2016
	OMB issues updated M-07-16		March 31, 2016		
Objective 4: Human Resources	Agencies report all cyber positions to OPM	December 31, 2015			
	Study of Federal cyber workforce delivered to CIO Council			April 30, 2016	
Objective 5: Technology	CIO Council establishes subcommittee on rapid deployment of emerging technology	December 31, 2015			

PMC Quarterly Assessment | PMC Quarterly Assessment | PMC Quarterly Assessment | PMC Quarterly Assessment | PMC Quarterly Assessment

*Note: This timeline provides only a sampling of key actions and milestones outlined in the CSIP

FY16 OMB FISMA Guidance

- Last week, OMB issued memo with guidance for FY16 FISMA reporting, under FISMA 2014.
- "As a result of cyber incidents impacting Government information that resides on or is connected to contractor systems, a group of experts in security, privacy, and the Federal acquisitions process were tasked with reviewing existing contract clauses and providing recommendations…"
  - To be released in Q1 FY16.
  - "Provides clarity around requirements for security in Federal acquisitions."

Revision to OMB Circular A-130

- First revision in 15 years.
- "[P]rovides general policy for the planning, budgeting, governance, acquisition, and management of Federal Information resources."
- Revised Appendix III "provides guidance on agency information security and privacy management, including the transition from the current periodic point-in-time authorization process to a more dynamic continuous monitoring . . ."
- Draft released October 21; 30 day comment period.

Interim DFARS Rule: Network Penetration Reporting/Cloud Computing

- Contractors and subcontractors are required to:
  - Safeguard covered defense information residing in or transiting through covered contractor information systems by applying network security controls.
  - Report cyber incidents.
- Required flow-downs for subcontractors at all tiers.
- Effective immediately upon issuance.
- DoD already issued class deviation for multi-factor authentication, allowing nine months from award to comply.

Interim DFARS Rule: Security Controls

- **Not part of IT service or system.** Comply with security requirements in NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations or equally effective alternate, approved in writing pre-award.
- **Part of non-cloud IT service/system.** Subject to security requirements specified in contract.
- **Part of cloud IT service/system.** Controls with security level and services required in accordance with DoD Cloud Computing Security Requirements Guide, and maintain data in U.S.

Interim DFARS Rule: Incident Reporting

- Report to DoD within 72 hours of discovery of incident affecting covered system, or that affects contractor's ability to perform operationally.
- Subcontractors report to DoD ***and*** prime.
- Submit any malware to CO.
- Preserve images, relevant monitoring/packet capture data, for at least 90 days.
- Upon request, provide DoD with access to information and equipment, and damage assessment.

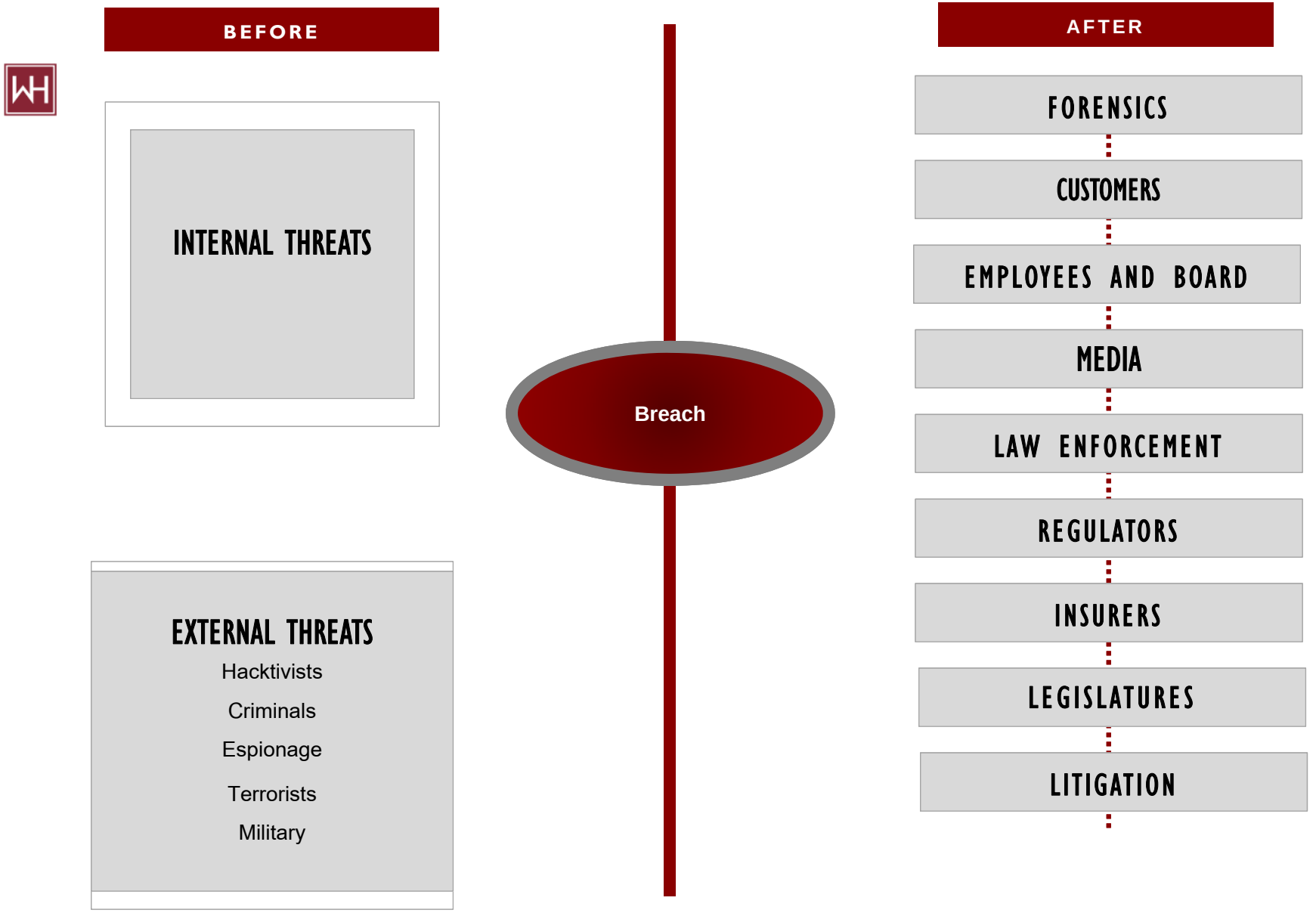
Implications of Interim DFARS Rule

- Category of information/systems subject to rule is loosely defined – quite broad.
- NIST security standards are highly detailed and can be quite onerous.
  - Especially burdensome for smaller contractors or lower-tier subcontractors.
  - Some recognition of this by DoD with class deviation for MFA.
- False Claims Act?

Breach Preparedness and Response

A. Overview: Cyber Threat Landscape and Breach Response
B. Incident Response Planning
C. Managing Breach Response
D. Breach Notification Requirements for Government Contractors

Cyber Threat Landscape and Breach Response



Some Lessons from the Field: IT Practices

Overall Management

•Failure to address recommendations from third-party assessments
•Unbalanced risk assessment process

Identity and Access Management

•Lack of control over system administrator credentials
•Use of default passwords for privileged accounts
•Improper/unnecessary access to networks by third-parties

Data Protection

- Lack or failure of encryption
- Incomplete inventory of sensitive data and its locations, leading to insufficient protection for the data

Infrastructure Security

- Improper segmentation
- Failed or insufficient network monitoring
- Unnecessary permissions for connections between severs
- Failure to decommission systems no longer in use
- Unnecessary connection between servers and the external internet
- Failure to deploy purchased network security/monitoring tools

Application Security

- Application patching and updating problems
- Failure to restrict permissions to install unauthorized software
- Failure to audit for known vulnerabilities

Incident Response Planning

Effective data breach response <u>requires</u> pre-breach preparation

- Written incident response plan:
  - ✓ Identify 24/7 points of contact
  - ✓ Establish clear roles and responsibilities
  - ✓ Provide escalation procedures
  - ✓ Account for different types of incidents
  - ✓ Give guidance on responding to customers, business partners, press, regulators, and others
  - ✓ Reflect notice and reporting requirements
- Ideally includes tabletop exercises or roleplaying a simulated breach
- Negotiation of engagement terms with data forensic firm(s)
- Engagement of other vendors necessary for effective breach response
- Contingency plans for providing notice to customers

Managing Breach Response

Understand the Incident and Prevent Further Exploitation

- ✓ Conduct a legally privileged investigation
- ✓ What happened and has the breach been stopped
- ✓ How significant is the threat to business
- ✓ First reports are often incorrect/incomplete

Communications Issues

- ✓ Prioritize reputational issues
- ✓ Consider all audiences
- ✓ Consider what you know and do not know
- ✓ What is the core narrative?

Legal Issues

- ✓ Consider legal privilege for all post-breach actions
- ✓ Identify financial control systems ASAP; include in scope of forensic work
- ✓ Address regulators and law enforcement
- ✓ Evaluate legal notification and disclosure requirements
- ✓ Be mindful of potential litigation
- ✓ Insurance

Some Key Takeaways on Breach Preparedness and Response

Pay Attention	• Cyber issues raise legal concerns throughout the enterprise. Be aware of evolving regulatory requirements and expectations.
Be Prepared	• Develop a comprehensive, integrated incident response plan.
Manage Your Response	• Assemble an experienced team—including legal and non-legal components—to ensure breach response is integrated and effective

Notification & Reporting Requirements

Government contractors and subcontractors are subject to multiple, overlapping cybersecurity and privacy breach notification and reporting regimes.

- Personal information
- Government information
- Defense/security information

Notification & Reporting Requirements: Personal Information

- State personal data breach laws
  - Mandatory notifications in 47 states, DC, PR, and territories
  - Different formulations of “personal” information
  - Different breach triggers
  - Different regulatory, attorney general, and media reporting rules
- Federal sector-specific notification requirements
  - HIPAA/HITECH Act: Unsecured protected health information
  - Financial institution notification under Gramm-Leach-Bliley guidance

Notification & Reporting Requirements: Government Information

- FAR 52.239-1(c): Report “new or unanticipated threats or hazards” or “if existing safeguards have ceased to function.”
- FISMA
  - Report breaches and incidents per System Security Plan
  - Report security issues in Plan of Action & Milestones (POAM)
- FedRAMP
  - Contract guidance envisions reporting of security incidents to US-CERT

Notification & Reporting Requirements: Defense/security information

- Classified information
  - Report loss, compromise, or suspected compromise to cognizant security officer
  - Report suspected espionage to FBI
- DFARS 252.204-7012
  - Applies to “cyber incidents”
  - Report within 72 hours of discovery
  - Mandatory flowdown to subcontractors

Notification & Reporting Requirements: Defense/security information

- Defense Industrial Base Cybersecurity/Information Assurance (DIB CS/IA) Program
  - Expands mandatory “cyber incident” reporting effective October 2, 2015
  - Applies to all DoD contracts and agreements; mandatory flowdown
  - Open for comments until December 1, 2015
- Nexus with export control
  - Mandatory disclosure to DoD may reveal lapses in security that implicate export control laws and regulations

Questions?

Jonathan Cedarbaum
Partner
+1 202 663 6315
jonathan.cedarbaum@wilmerhale.com

Barry Hurewitz
Partner
+1 202 663 6089
barry.hurewitz@wilmerhale.com

Ben Powell
Partner
+1 202 663 6770
benjamin.powell@wilmerhale.com

Leah Schloss
Associate
+1 202 663 6481
leah.schloss@wilmerhale.com

Jason Chipman
Counsel
+1 202 663 6195
jason.chipman@wilmerhale.com

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is not approved for New York newly admitted attorneys. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Please note that no partial credit will be awarded. Attendees requesting CLE credit must attend the entire program.