



29TH ANNUAL OUNCE OF PREVENTION SEMINAR

Weathering the
Rough Seas of
Regulation



Managing the Cyber Threat Crisis

Cyber Threats & Enforcement Risks for
Corporate Boards & Officers

David Z. Bodenheimer



Digital Pearl Harbor

DoD Secretary
Panetta



“cyber Pearl Harbor” (2012)

DHS Secretary
Napolitano



“cyberattack” data like 9/11 (2012)

FBI Director
Mueller



“greatest threat to our country” (2012)

Cyber Theft & Espionage: Why Corporate Boards & Officers Need to Worry Now



Secrets
Gone?



122

Cyber Theft & Espionage



- Intelligence Warnings
- The loss of intellectual property due to cyber attacks amounts to the “greatest transfer of wealth in human history.”
- (Gen. Keith Alexander, U.S. Cyber Command Chief & NSA Director, July 2012)
- More Warnings
- Counterintelligence Executive Report (Oct. 2011)
- GAO Report & Testimony (June 2012)
- Defense Security Service Trend Analysis (2012)
- National Intelligence Estimate (2013)
- Mandiant Investigative Report (2013)

Foreign Cyber Threats



- 40,000 Hackers: “There are forty thousand Chinese hackers who are collecting intelligence off U.S. information systems and those of our partners.” (Adm. McConnell, Jan. 2008)
- Daily Attacks. “A defence force source said yesterday that attacks initiated from China occurred almost on a daily basis.” (Australian Defense Force, Apr. 2009)
- Classified Data Compromised. “A China-based cyber espionage network had accessed 1200 computers in 103 countries containing classified documents.” (Munk Centre for Int’l Studies, Apr. 2009)
- China’s Cyber Spy House



FIGURE 7: Unit 61398 Center Building 208 Datong (rear view, possible generator exhausts visible) Image Copyright 2013 city8.com

Data Losses & Cyber Breach

- 2x Library of Congress
- → 38 terabytes of lost data
- “As an example of the threat, one American company had 38 terabytes of sensitive data and intellectual property exfiltrated from its computers – equivalent to nearly double the amount of text contained in the Library of Congress.”
- [Sen. Whitehouse, May 10, 2010]
- It’s Personal
- “As an example, in 2008, [China’s] APT1 compromised the network of a company involved in a wholesale industry. . . . Over the following 2.5 years, APT1 stole an unknown number of files from the victim and repeatedly accessed the email accounts of several executives, including the CEO and General Counsel.”
- [Mandiant Report (Feb. 2013)]



IP Cyber Losses



- One Company's IP Loss
- "For example, a 2011 FBI report noted, "company was the victim of an intrusion and lost 10 years' worth of research and development data –valued at \$1 billion – virtually overnight."
- CRS Report, 2013
Cybersecurity Executive Order (Mar. 2013)
- \$1 Trillion IP Losses
- "Last year alone, cyber criminals stole intellectual property from businesses worldwide worth up to \$1 trillion." (President Obama, 2009)



Stock Price Losses



- Investors Really Care
- 70% of investors – interested in reviewing corporate cyber practices
- 80% of investors – likely would not invest if history of cyber attacks
- Zogby Analytics Survey (Mar. 2013)
- Stock Prices Hammered
- 9% Stock Loss – after Global Payments breach (before trading halted)
- 84% Stock Loss – after Chinese firm took AMSC's source code



127

Cybered M&A Deals



- Infiltrated M&A Deals
- \$2.4 Billion Huiyuan Deal. Coca Cola's deal collapsed after hackers took key files
- \$40 Billion BHP Deal. BHP Billiton Ltd's bid to acquire Potash Corp. collapsed after cyber theft
- "Coke Gets Hacked and Doesn't Tell Anyone," Bloomberg.com (Nov. 2012)
- Nat. Counter Intel Report
- "Information was pilfered from the corporate networks of a US Fortune 500 manufacturing company during business negotiations in which that company was looking to acquire a Chinese firm [T]his may have helped the Chinese firm attain a better negotiating and pricing position." [National Counter-intelligence Executive, Oct. 2011]

Cybered Negotiations



- \$1.3 Billion Left on Table
- “In one case, officials estimated the cost of lost data from a British company . . . Jonathan Evans, head of Britain’s MI5 domestic security service, said . . . digital intruders targeting a ‘major London listed company’ had caused a loss of 800 million pounds (\$1.3 billion), in part because of the resulting disadvantage in ‘contractual negotiations.’”
- “China-Based Hacking of 760 Companies Shows Cyber Cold War,” Bloomberg.com (Dec. 2011)
- Double-Digit Losses
- After China’s APT1 compromised the network of a company in the wholesale industry, “major news organizations reported that China had successfully negotiated a double-digit decrease in price per unit with the victim organization for one of its major commodities.”
- Mandiant Report (Feb. 2013)

Cybered Operations

- 30,000 Dead Computers
- “In August 2012, a series of cyber attacks were directed against Saudi Aramco, the world’s largest oil and gas producer and most valuable company. The attacks compromised 30,000 of the company’s computers and the code was apparently designed to disrupt or halt the production of oil.”
- [CRS, 2013 Cybersecurity Executive Order, Mar. 2013]
- Iranian Cyber Attacks
- Bank of America & J.P. Morgan Chase Cyber Attacks. “I don’t believe these were just hackers,” [Sen.]Lieberman said “I believe this was done by Iran and the Qods force, which has its own developing cyber attack capacity.”
- “In a ‘highly classified’ report last week the Joint Chiefs of Staff’s Intelligence Directorate, or J-2, confirmed continuing Iranian cyber attacks against U.S. financial institutions, NBC said.”
- [Matt Egan, FoxBusiness, Sept. 24, 2012]



How Do You Know When Your Company is a Cyber Target?



Who's a Cyber Target?



- McAfee Survey
 - 60% reported “chronic and recurring loss” of sensitive information
- CSIS Report
 - 85% energy/power sector experienced “network intrusions”
- Mandiant Report
 - 141 companies in 20 major industries compromised by cyber intrusions (Mandiant Report)
- 2 Types of Companies
- “There are only two types of companies: Those that have been hacked, and those that will be. Even that is merging into one category: Those that have been hacked and will be again.”
- FBI Director
- Robert Mueller
- (Mar. 2012)



Who's a Cyber Target?



- Top Cyber Targets
- Information Technology
- Communications
- Military Technology
- Aerospace
- Dual Use Technology
- Healthcare & Pharma
- Agricultural Technology



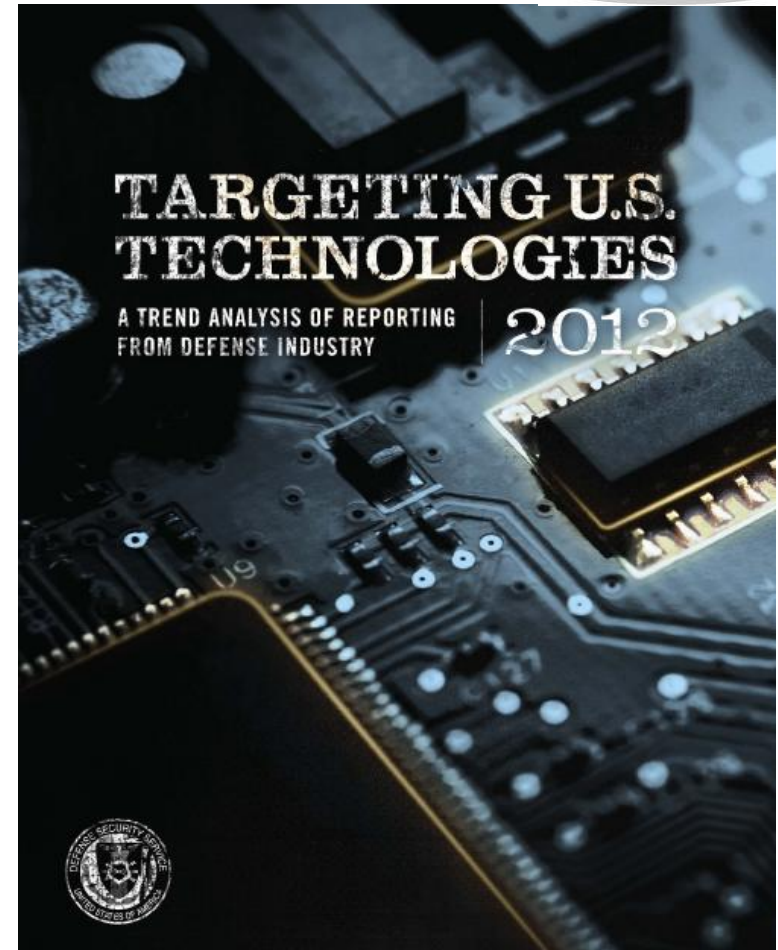
133

Who's a Cyber Target?



TOP TARGETED TECHNOLOGIES*

-  INFORMATION SYSTEMS
-  LASERS, OPTICS, AND SENSORS
-  AERONAUTICS SYSTEMS
-  ELECTRONICS
-  ARMAMENTS AND ENERGETIC MATERIALS
-  SPACE SYSTEMS
-  MARINE SYSTEMS
-  POSITIONING, NAVIGATION, AND TIME
-  MATERIALS AND PROCESSES
-  GROUND SYSTEMS
-  INFORMATION SECURITY
-  PROCESSING AND MANUFACTURING



Who's Attacking Who?



Who are the Hackers?

- Foreign Nations →
- Organized Crime →
- Terrorists →
- Hactivists →
- Hackers for Hire →

What are the Targets?

- Cyber Espionage (IP)
- ID Theft (personal data)
- Critical Infrastructure
- Political Disruption
- All of the Above



Who Are the Enforcers Coming After You – After a Security Breach?



Secrets
Gone?



Cyber Risks – SEC Scrutiny

- SEC Scrutiny
- - Disclose material risks?
- Impact
- → SEC scrutiny or actions
- “Cyber risk management is a critical corporate responsibility. Federal securities law requires publicly traded companies to disclose ‘material’ risks and events, including cyber risks and network breaches. A review of past disclosures suggests that a significant number of companies are failing to meet these requirements.” [Senate Commerce News Release, May 12, 2011]
- SEC Disclosure Duty
- Division of Corporation Finance Securities and Exchange Commission
- CF Disclosure Guidance: Topic No. 2 Cybersecurity
- Date: October 13, 2011
- Summary: This guidance provides the Division of Corporation Finance's views regarding disclosure obligations relating to cybersecurity risks and cyber incidents
- Disclosure Duties
- Risk of Cyber Incidents
- Prior Security Breaches
- Adequacy of Preventative Measures



Cyber Risks – Shareholders

- Disclose Risks – Or Not?
- Rock & a Hard Place?
- \$20 Million Suit. Countrywide’s lax “internal procedures” & security breach [Courthouse News, Apr. 5, 2010]
- \$7.2 Million/Incident. “average cost of a data breach hit \$7.2 million last year” [NYT, Dec. 2011]
- Shareholder Actions
- Delaware case law (corporate director’s good faith duties re information & reporting systems, plus potential liability for damages)
- National Counterintelligence Executive Report (Oct. 2011)

138

Cyber Risks – Congress

- Congressional Inquiry
- Sen. Rockefeller's Letter
- 300 CEOs Responded
- Did Your CEO Respond?
- What did your CEO say?
- Is your company doing it?
- Will a plaintiff get hold of it?

JOHN D. ROCKEFELLER III, WEST VIRGINIA, CHAIRMAN

DANIEL K. ROBYNE, IOWA	KAY DAILY HATZIGOSIN, TEXAS
JOHN F. KERRY, MASSACHUSETTS	ELI WHIPPLE, ILLINOIS, MAINE
BARBARA ROSEN, CALIFORNIA	JIM R. BARRÉ, SOUTH CAROLINA
THE HONORABLE RICHARD	JOHN F. BARRÉ, SOUTH CAROLINA
MARIA CANTWELL, WASHINGTON	ROBERT F. WALKER, MISSISSIPPI
FRANK R. LAUTENBERG, NEW JERSEY	JOHN W. BLANKEN, GEORGIA
MIKE PENCE, INDIANA	ROY BLUNT, MISSOURI
CLAYPE W. CASSELL, MISSOURI	JOHN BOZMAN, MONTANA
GARY ALBERICIANI, WISCONSIN	PATRICK J. TOOMEY, PENNSYLVANIA
TOM COONS, WASHINGTON	MARCO RUBIO, FLORIDA
MARK WARREN, UTAH	KELLY AYOTTE, NEW HAMPSHIRE
MAT KOTTE, ALASKA	DEAN DILLON, NEVADA

ELI WHIPPLE, STAFF DIRECTOR
 BRUCE M. HORNBERG, REPUBLICAN STAFF DIRECTOR AND GENERAL COUNSEL

United States Senate
 COMMITTEE ON COMMERCE, SCIENCE,
 AND TRANSPORTATION
 WASHINGTON, DC 20510-6125
 Web site: <http://commerce.senate.gov>
 September 19, 2012

Fortune 500 CEO USA

I was profoundly disappointed that the United States Senate's effort to pass comprehensive cybersecurity legislation was blocked by a partisan filibuster last month. The cyber threats we face are real and immediate, and Congress's failure to pass legislation this year leaves the country increasingly vulnerable to a catastrophic cyber attack. Because of the urgency of the need to address this threat, in August following the Senate's failure to act, I urged President Obama to use his authority to implement cybersecurity protections for our country through an Executive Order.

To help me understand your company's views on cybersecurity, I ask that you provide responses to the following questions by Friday, October 19, 2012.

1. Has your company adopted a set of best practices to address its own cybersecurity needs?
2. If so, how were these cybersecurity practices developed?
3. Were they developed by the company solely, or were they developed outside the company? If developed outside the company, please list the institution, association, or entity that developed them.

Cyber Risks – DoD Contracts

- NDAA § 941
- - “cleared defense contractors”
- “Rapid Reporting”
- “technique or method use in such penetration”
- “sample of malicious software”
- “summary of information . . . potentially compromised”
- DoD “Access”
- DoD access to contractor network & data for forensics analysis
- Limited purpose & trade secrets

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2013

SEC. 941. REPORTS TO DEPARTMENT OF DEFENSE ON PENETRATIONS OF NETWORKS AND INFORMATION SYSTEMS OF CERTAIN CONTRACTORS.

(a) PROCEDURES FOR REPORTING PENETRATIONS.—The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

(b) NETWORKS AND INFORMATION SYSTEMS SUBJECT TO REPORTING.—

(1) RAPID REPORTING.—The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection (b). Each such report shall include the following:

(A) A description of the technique or method used in such penetration.

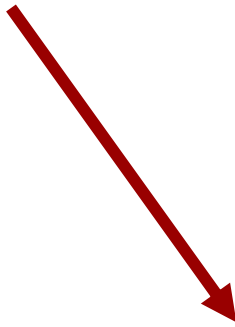
(B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration.

(C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

(2) ACCESS TO EQUIPMENT AND INFORMATION BY DEPARTMENT OF DEFENSE PERSONNEL.—The procedures established pursuant to subsection (a) shall—

Cyber Risks – Executive Order

- Information Sharing
- → Should you be sharing?
- Yes?
- Critical for identifying threats
- Essential tool for cybersecurity
- No? -- Safe Harbors?
- Investigation due to reporting?
- Lawsuit triggered by sharing?
- Antitrust issue for B-2-B sharing?



- Executive Order

The White House

Office of the Press Secretary

For Immediate Release

February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

Sec. 4. Cybersecurity Information Sharing. (a) It is the policy of the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats. Within 120 days of the date of this order, the Attorney General, the Secretary of Homeland Security (the "Secretary"), and the Director of National Intelligence shall each issue instructions consistent with their authorities and with the requirements of section 12(c) of this order to ensure the timely production of unclassified reports of cyber threats to the U.S. homeland that identify a specific targeted entity. The instructions shall address the need to protect intelligence and law enforcement sources, methods, operations, and investigations.

Cyber Risks – Info Sharing


- Sharing Data with Feds
- What do you say when the Feds come knocking?
 - - Authority to share data?
 - - Potential 3rd party liability?
 - - Privacy issues?
- Potential Exposure
 - - Attorney-client privilege?
 - - FOIA protection?
 - - Use for other investigations?
-
- \$50 Billion Lawsuit
- “One lawsuit alone, filed May 12 by a purported national class of Verizon customers, seeks \$50 billion in damages.”
- [“Court Will Decide State Secrets Issues First in NSA Phone Surveillance Class Action Suit,” Privacy Law Watch, June 9, 2006]



Cyber Risks – FCA Actions

- Cyber Fraud Risks
- - What did you tell the Federal agency?
- Failed Cybersecurity
- → False Claims Act suit
- “PLASTILAM, INC. failed to take sufficient steps to safeguard confidential data, including the names and Social Security numbers of over 100 Medicare beneficiaries. The investigation revealed that a number of misprinted beneficiary cards were discarded, whole, in an unsecured dumpster.”



 The United States Attorney's Office
District of Massachusetts

FOR IMMEDIATE RELEASE
JUNE 7, 2010
WWW.USDOJ.GOV/USAO/MA
E-MAIL: USAMA.MEDIA@USDOJ.GOV

SALEM PRINTING BUSINESS TO PAY \$25,000 FOR IMPROPER DATA SECURITY PRACTICES AND DISPOSAL OF MEDICARE BENEFICIARY CARDS

BOSTON, Mass. - The United States has reached a settlement with a Salem printing business in connection with potential civil penalty claims under the False Claims Act. United States Attorney Carmen M. Ortiz and J. Anthony Ogden, Inspector General of the United States Government Printing Office (GPO-OIG), announced today that PLASTILAM, INC., a printing business located in Salem, Mass., has reached a settlement with the Government, in connection with potential civil penalty claims under the False Claims Act, investigated by GPO-OIG and the U.S. Attorney's Office.

Based upon facts developed in the course of the investigation, the United States contended that between August 2007 and August 2008, while working on a GPO contract to produce plastic Medicare beneficiary cards, PLASTILAM, INC. failed to take sufficient steps to safeguard confidential data, including the names and Social Security numbers of over 100 Medicare beneficiaries. The investigation revealed that a number of misprinted beneficiary cards were discarded, whole, in an unsecured dumpster. These cards were later scattered around a local park by area children before being recovered by local police.

PLASTILAM, INC. has agreed to pay \$25,000 in settlement of the United States' penalty claims, without admitting wrongdoing or liability. Based upon the Government's investigation, it does not appear that any of the improperly safeguarded information was released deliberately, nor does it appear that any of the data was misused or stolen.

"We are committed to protecting the public by holding federal contractors who handle sensitive personal data, to the highest standards," said U.S. Attorney Ortiz. "Contractors who work with sensitive data must exercise vigilance in handling these materials. They must understand that even those data breaches are not due to deliberate misconduct, will be swiftly investigated and met with appropriate consequences."

Inspector General Ogden said, "The GPO OIG takes seriously allegations of improper conduct by GPO contractors, especially those responsible for the handling and protection of sensitive information, such as citizens' personally identifiable information (PII). I applaud the efforts of our investigators and the Department of Justice in bringing this matter to a meaningful resolution. While this is just one in a series of contract investigations our office is pursuing, this settlement should send a message that the breach of data security requirements and the compromise of PII will not be tolerated, and that we will hold accountable those administering and performing contracts for GPO."

The investigation leading to the settlement was conducted by the Office of the Inspector General of the U.S. Government Printing Office. It was prosecuted by Assistant U.S. Attorney Zachary A. Cunha of Ortiz's Civil Division.

Questions?

David Bodenheimer

(202) 624-2713

dbodenheimer@crowell.com

"Securing cyberspace is one of the most important and urgent challenges of our time."

Senator Jay Rockefeller, Chairman of the Senate Commerce, Science and Transportation Committee

May 2011

CF Disclosure Guidance: Topic No. 2

- Corporation Finance issues guidance October 13, 2011
- Deliberate attacks or unintentional events
- Theft of financial assets, intellectual property, or other sensitive information belonging to registrants

CF Disclosure Guidance: Topic No. 2

- Remediation costs
- Increased cybersecurity protection costs
- Lost revenues
- Litigation
- Reputational damage adversely affecting customer or investor confidence

CF Disclosure Guidance: Topic No. 2

- Material risks
- Cyber incidents
- Cyber incidents that may be undetected
- Insurance coverage

SEC – Big 6

- Risk factors
- MD&A
- Description of business
- Legal proceedings
- Financial Statement disclosures
- Disclosure Controls & Procedures

Evolution of Disclosure

- Facebook
- Comment Letters
 - Disclose specific cybersecurity breaches
 - Cybersecurity risks should stand alone
 - All material breaches should be disclosed
- Recent Form 10-K Disclosures

Why Do Shareholders Care?

- Key current issue
- Costs
- Company value
- Litigation

Board of Directors

- The Tone is set at the Top
- Risk Management
- Insurance
- Business Judgment Rule & Fiduciary Duties
- Officers

Cyber Threats and Due Diligence

- Increased focus in transactions
- Understanding the risks
- Key component of company value

Conclusions

- Key business issue
- SEC focus
- Costs
- Liability
- Best practices flowing down to private companies

Questions?

Bryan Brewer

(202) 624-2605

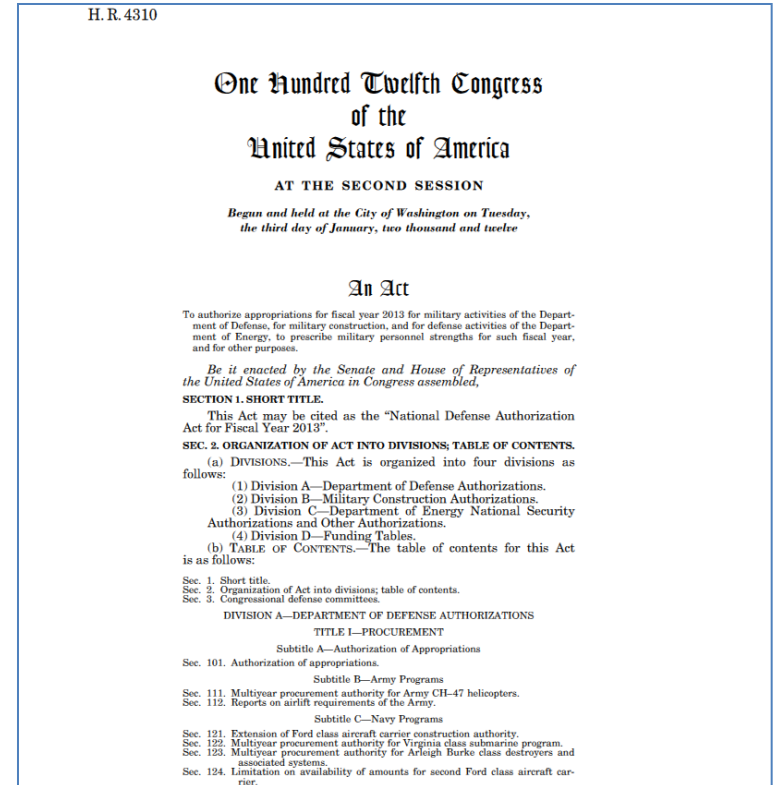
bbrewer@crowell.com

Managing the Cyber Threat Crisis New Rules, Regulations and Solicitations

Gordon Griffin

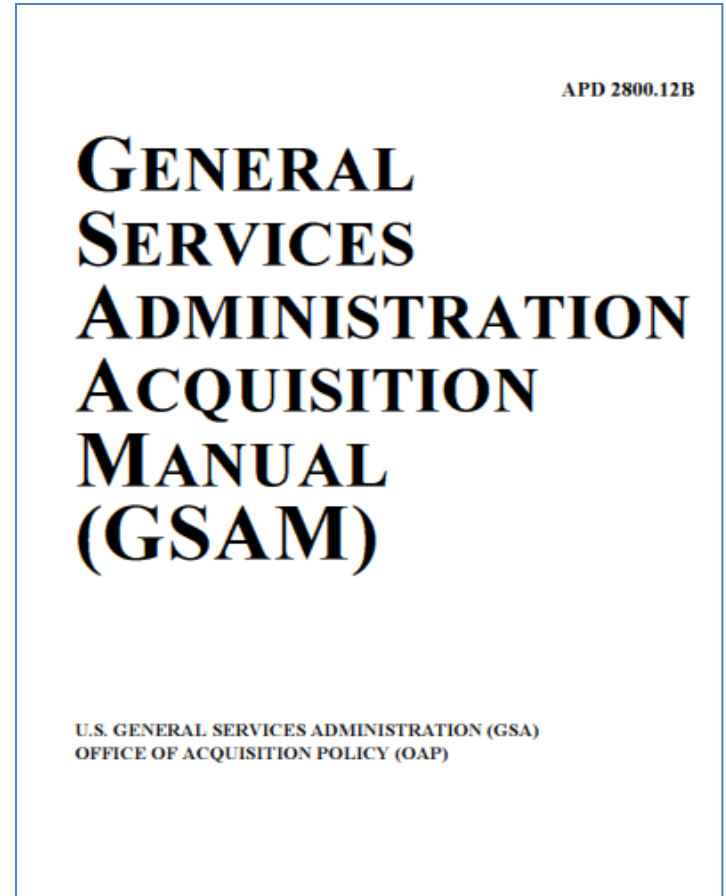
Audits

- “[DOD regulations] shall include mechanisms for Department of Defense personnel to, upon request, obtain access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor.”



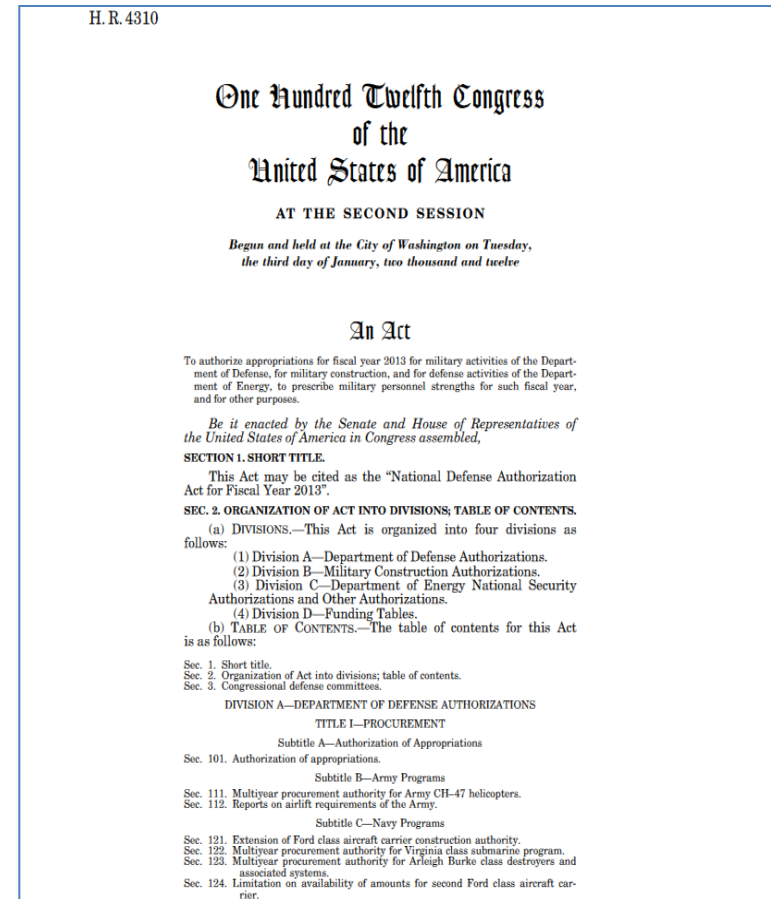
Audits - Continued

- “The Contractor shall afford GSA access to the Contractor’s and subcontractors’ facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location. Access shall be provided to the extent required, in GSA’s judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of GSA data or to the function of information technology systems operated on behalf of GSA, and to preserve evidence of computer crime.”



Breach Notification

- “The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.”



Continuing Resolution – Supply Chain

- Sec. 516. (a) None of the funds appropriated or otherwise made available under this Act may be used by the Departments of Commerce and Justice, the National Aeronautics and Space Administration, or the National Science Foundation to acquire an information technology system unless the head of the entity involved, in consultation with the Federal Bureau of Investigation or other appropriate Federal entity, has made an assessment of any associated risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China.

160

One Hundred Thirteenth Congress
of the
United States of America

AT THE FIRST SESSION

*Began and held at the City of Washington on Thursday,
the third day of January, two thousand and thirteen*

An Act

Making consolidated appropriations and further continuing appropriations for the
fiscal year ending September 30, 2013, and for other purposes.

*Be it enacted by the Senate and House of Representatives of
the United States of America in Congress assembled,*

SHORT TITLE

SECTION 1. This Act may be cited as the "Consolidated and
Further Continuing Appropriations Act, 2013".

TABLE OF CONTENTS

SEC. 2. The table of contents of this Act is as follows:

Sec. 1. Short title.
Sec. 2. Table of contents.
Sec. 3. References.
Sec. 4. Explanatory statement.
Sec. 5. Availability of funds.

DIVISION A—AGRICULTURE, RURAL DEVELOPMENT, FOOD AND DRUG
ADMINISTRATION, AND RELATED AGENCIES APPROPRIATIONS ACT, 2013

Title I—Agricultural Programs
Title II—Conservation Programs
Title III—Rural Development Programs
Title IV—Domestic Food Programs
Title V—Foreign Assistance and Related Programs
Title VI—Related Agency and Food and Drug Administration
Title VII—General provisions

DIVISION B—COMMERCE, JUSTICE, SCIENCE, AND RELATED AGENCIES
APPROPRIATIONS ACT, 2013

Title I—Department of Commerce
Title II—Department of Justice
Title III—Science
Title IV—Related agencies
Title V—General provisions

DIVISION C—DEPARTMENT OF DEFENSE APPROPRIATIONS ACT, 2013

Title I—Military Personnel
Title II—Operation and Maintenance
Title III—Procurement
Title IV—Research, Development, Test and Evaluation
Title V—Revolving and Management Funds
Title VI—Other Department of Defense Programs
Title VII—Related agencies
Title VIII—General provisions
Title IX—Overseas contingency operations

DIVISION D—DEPARTMENT OF HOMELAND SECURITY APPROPRIATIONS
ACT, 2013

Title I—Departmental management and operations

HIPAA Regulations

- January 25, 2013, HIPAA Rule makes several changes:
 - Breach Notification Rule
 - Security Rule
 - Business Associate Liability

Violation category—Section 1176(a)(1)	Each violation	All such violations of an identical provision in a calendar year
(A) Did Not Know	\$100–\$50,000	\$1,500,000
(B) Reasonable Cause	1,000–50,000	1,500,000
(C)(i) Willful Neglect-Corrected	10,000–50,000	1,500,000
(C)(ii) Willful Neglect-Not Corrected	50,000	1,500,000

Liquidated Damages & Penalty Provisions

- HHS Solicitation:
 - “In the event of a breach, the contractor shall be liable for \$500 per effected user. The contractor shall be liable for the Government’s costs to notify and/or remediate the breach of private personal data with FOH customers. Based on the nature of the breach, the Government shall define a remediation plan, and the contract shall support the defined actions. In addition to restitution for the labor efforts to coordinate the notification, this remediation shall include the cost of providing credit protection to all effected people.”

Solicitations

- CMS – State Based Exchanges
 - “The Business Associate shall report any violation in use or disclosure involving PHI or any security incident to CMS within one (1) hour of discovery in accordance with the ‘CMS Guide for the Incident Reporting Process.’”

Solicitations – Continued

- GSA – Occupational Health Review
 - “The Contractor shall comply with GSA Order CIO 2100.1 GSA Information Technology (IT) Security Policy and GSA Order ADM 9732.1D Suitability and Personnel Security. GSA separates the risk levels for personnel working on Federal computer systems into three categories: Low Risk, Moderate Risk, and High Risk. Criteria for determining which risk level a particular contract employee falls into are shown in Figure A-1 of GSA Order ADM 9732.1D.”

Solicitations – Continued

- Department of Commerce – Document Destruction
 - “The contractor shall afford DOC, including the Office of Inspector General, access to the contractor's and subcontractor's facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DOC data or to the function of computer systems operated on behalf of DOC, and to preserve evidence of computer crime.”

Solicitations – Continued

- HHS – Rx Database
 - “This contract requires the Contractor to develop, host, and/or maintain a Federal information system at the Contractor’s or any subcontractors’ facility. The Contractor shall submit an annual information security assessment using NIST SP 800-53, Recommended Security Controls for Federal Information Systems. The assessments shall be due annually within 30 days after the anniversary date of the contract, with the final assessment due at contract completion.”

Solicitations – Continued

- Department of Commerce – NIST Enterprise
 - “Contract employees may be barred from working on the premises of a facility for any of the following:
 - (3) Improper Conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct directly related to the contract.”

Questions?

Gordon Griffin

(202) 624-2819

ggriffin@crowell.com