THE GOVERNMENT CONTRACTOR®

WEST®

Information and Analysis on Legal Aspects of Procurement

Vol. 55, No. 24 **June 26, 2013**

Focus

¶ 198

FEATURE COMMENT: Regulating Cybersecurity On A Piecemeal Basis—Can The Executive Order Harmonize The Cyber Law Patchwork?

Driven by relentless cyber attacks stealing billions of dollars of U.S. technology and breaching the privacy of millions of Americans, the race is on to regulate cybersecurity in the public and private sectors. The hard question is how. The failure of Congress to pass comprehensive cybersecurity legislation in the last two years has a direct bearing upon this race to regulate.

On one hand, President Obama sought to fill this void with EO 13636, "Improving Critical Infrastructure Cybersecurity." 78 Fed. Reg. 11739 (2013). This order seeks to build a "cybersecurity framework" to "align" cybersecurity approaches in the public and private sectors, and to "harmonize and make consistent" cyber requirements for federal procurements. Id. at 11741–42. To implement the executive order's quest for "harmonized" cybersecurity standards, the General Services Administration and Department of Defense Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition issued a request for information (RFI) on May 13. 78 Fed. Reg. 27966–68 (2013). This RFI specifically seeks information on conflicting cyber standards and requirements:

> *Harmonization*: In general, DoD and GSA seek information about any conflicts in statutes, regulations, policies, practices, contractual terms and conditions, or acquisition processes affecting federal acquisition requirements related to cybersecurity and how the federal government might address those conflicts.

On the other hand, the lack of comprehensive cybersecurity legislation has created a legal vacuum that has been filled with an ad hoc, sector-by-sector approach to regulating cybersecurity through narrowly targeted federal statutes, regulations and policies. Over the past two years, a few examples include:

- Defense Contractors. The most recent National Defense Authorization Act established requirements for certain defense contractors to report security breaches and provide security audit access.
- Public Companies. The Securities and Exchange Commission issued guidelines for public companies to report on material incidents involving security breaches and cybersecurity safeguards.
- Information Technology Companies. For certain federal agencies buying IT systems, Congress has prohibited such acquisitions unless the Federal Bureau of Investigation has made a risk assessment regarding the potential for "cyber-espionage or sabotage" by the People's Republic of China.
- Health Care Sector. The Department of Health and Human Services published new information security rules and breach notification obligations for the health care sector.
- Critical Infrastructure Sectors. The new executive order calls for a framework for standards for the critical infrastructure sectors, but many already have their own information security requirements and standards that may slow the drive towards common standards.

These recent trends in regulating information security on a piecemeal basis underscore the challenges ahead for the executive order policy to "align" and "harmonize" cybersecurity standards and requirements. Both public- and private-sector entities need to understand these trends towards regulating cybersecurity with a patchwork of cyber laws and regulations, as well as the impact of attempting to comply with multiple cyber standards coming from many directions.

Recent Trends in Patchwork Regulation of Cybersecurity—Over the past few years, Congress has been busy with a host of cybersecurity bills, including "several dozen cybersecurity-related bills before Congress" in 2010 alone. Sen. Sheldon Whitehouse (D-R.I.), "We Need to Act on Cybersecurity," *The National Law Journal* (May 10, 2010). But none of the comprehensive bills have passed.

Instead, Congress has targeted certain industries or niches of cybersecurity with narrow legislation. At the same time, federal agencies have regulated cybersecurity for specific sectors with their own regulations, rules and standards. As a result, both the public and private sectors need to keep track of the new requirements and emerging trends in cyber law and regulation.

Cyber Requirements for "Cleared Defense Contractors": In 2013, Congress imposed cybersecurity requirements specifically aimed at "cleared defense contractors," defined as "a private entity granted clearance by the Department of Defense to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the Department of Defense." National Defense Authorization Act for Fiscal Year 2013, P.L. 112-239, § 941 (2013).

Section 941 also defined "covered network," but did not limit the scope to classified networks: "The term 'covered network' means a network or information system of a cleared defense contractor that contains or processes information created by or for the Department of Defense with respect to which such contractor is required to apply enhanced protection." Federal contractors without a security clearance need not worry about § 941.

But for "cleared" defense contractors, this section leaves open the possibility that it may extend to both classified and *unclassified* networks. If unclassified networks also fall within the scope of § 941, then the provision could have expansive reach, potentially driving cyber requirements throughout a contractor's network and organization.

Section 941 established two basic requirements for securing networks and information systems of "each cleared defense contractor": (1) security breach notification requirements, and (2) security audit access to the networks of such military contractors. Security breach notification requirements already exist in some areas at both the federal and state levels. Now, § 941 adds yet another. Under this new reporting requirement, § 941 requires that covered defense contractors provide "rapid reporting" of successful penetrations of their networks and information systems:

> (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.

Just how "rapid" is not explained in this reporting requirement. DOD's implementing procedures will presumably provide more detailed guidance on how rapidly to report "successful penetrations" of such networks.

For this "rapid reporting," § 941 specifies that "[e]ach such report shall include the following":

- "A description of the technique or method used in such penetration,"
- "A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration," and
- "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."

Given such reporting requirements, covered defense contractors will need to react quickly by gathering forensic evidence and identifying the hacking tools used. In addition, § 941 includes a "harm" analysis that must address whether DOD information has been compromised by the successful penetration.

Not only must covered defense contractors satisfy the "rapid reporting" requirement, but they must also provide "access" rights for DOD to review their networks and information systems. The implementing DOD procedures will "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."

However, § 941 does impose some limitations on the scope of DOD's access: (a) the access must be limited to the purpose of determining whether a DOD program suffered an exfiltration of data, and (b) DOD must provide for reasonable protection of the contractor's trade secrets and other business data.

SEC Guidance for Publicly Traded Companies: On Oct. 13, 2011, SEC entered the race to regulate cybersecurity, identifying this area as a potential material risk for publicly traded companies. SEC, "Cybersecurity: CF Disclosure Guidance: Topic No. 2" (Oct. 13, 2011). In this guidance, SEC addressed certain risk factors that may trigger a corporate duty to make a public disclosure.

Impact of Cyber Attacks. As documented in a host of congressional hearings, Government investigations and private-sector reports, cyber attacks have done great damage to corporations of all sizes. In its guidance, SEC incorporated a panoramic list of potential injuries and impacts from cyber attacks and breaches that corporations may need to report:

> The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners. Registrants that fall victim to successful cyber attacks may incur substantial costs and suffer other negative consequences, which may include, but are not limited to:
>
> - Remediation costs that may include liability for stolen assets or information and repairing system damage that may have been caused. Remediation costs may also include incentives offered to customers or other business partners in an effort to maintain the business relationships after an attack;
> - Increased cybersecurity protection costs that may include organizational changes, deploying additional personnel and protection technologies, training employees, and engaging third party experts and consultants;
> - Lost revenues resulting from unauthorized use of proprietary information or the failure to retain or attract customers following an attack;
> - Litigation; and
> - Reputational damage adversely affecting customer or investor confidence.

Cyber Risk Assessment. Conducting a risk assessment of cyber threats represents a common element of an information security program. The SEC guidance underscores the importance for corporations to identify major threats and critical cyber risks that may affect their particular business:

> Registrants should disclose the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. [Footnote omitted.] In determining whether risk factor disclosure is required, we expect registrants to evaluate their cybersecurity risks and take into account all available relevant information, including prior cyber incidents and the severity and frequency of those incidents. As part of this evaluation, registrants should consider the probability of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption. In evaluating whether risk factor disclosure should be provided, registrants should also consider the adequacy of preventative actions taken to reduce cybersecurity risks in the context of the industry in which they operate and risks to that security, including threatened attacks of which they are aware.

Security Safeguards. Merely identifying and assessing the cyber threat is just one part of a corporation's cyber defenses. In addition, the SEC guidance instructs corporations to address security controls and any deficiencies that may increase exposure to cyber threats and security breaches:

> Registrants are required to disclose conclusions on the effectiveness of disclosure controls and procedures. To the extent cyber incidents pose a risk to a registrant's ability to record, process, summarize, and report information that is required to be disclosed in Commission filings, management should also consider whether there are any deficiencies in its disclosure controls and procedures that would render them ineffective. [Footnote omitted.] For example, if it is reasonably possible that information would not be recorded properly due to a cyber incident affecting a registrant's information systems, a registrant may conclude that its disclosure controls and procedures are ineffective.

Security Breaches. In the event of a material security breach, the SEC guidance specifies that corporations should address the impact in their public disclosures:

> For example, if material intellectual property is stolen in a cyber attack, and the effects of

> the theft are reasonably likely to be material, the registrant should describe the property that was stolen and the effect of the attack on its results of operations, liquidity, and financial condition and whether the attack would cause reported financial information not to be indicative of future operating results or financial condition. If it is reasonably likely that the attack will lead to reduced revenues [or], an increase in cybersecurity protection costs, including related to litigation, the registrant should discuss these possible outcomes, including the amount and duration of the expected costs, if material. Alternatively, if the attack did not result in the loss of intellectual property, but it prompted the registrant to materially increase its cybersecurity protection expenditures, the registrant should note those increased expenditures.

In summary, the SEC guidance on cybersecurity remains relatively new, with limited experience for corporations to apply the guidance and make public disclosures so far. Given the risk of major security breaches, the SEC guidance may ratchet up the pressure on companies to accelerate risk assessments and security safeguards to mitigate the risks of a major cybersecurity incident.

Supply Chain Security for Select Federal Agencies: Protecting the supply chain represents a fundamental element of a typical information security program. In the massive bill to continue funding federal agencies for 2013, Congress again took the ad-hoc approach to cybersecurity by regulating one piece of the supply chain. 2013 Consolidated and Further Continuing Appropriations Act, Division B, § 516(a), P.L. 113-6 (March 20, 2013).

This law applies not to the entire Federal Government, but just to select agencies buying products from Chinese entities:

> (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.
>
> (b) None of the funds appropriated or otherwise made available under this Act may be used to acquire an information technology system described in an assessment required by subsection (a) and produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China unless the head of the assessing entity described in subsection (a) determines, and reports that determination to the Committees on Appropriations of the House of Representatives and the Senate, that the acquisition of such system is in the national interest of the United States.

This patchwork surprise in § 516 raises a host of questions about its scope, meaning and intent.

- Why does it apply only to the departments of Commerce and Justice, NASA, and the National Science Foundation?
- May the "head of the entity" delegate the assessment of "any associated risk of cyber-espionage or sabotage"?
- What type of consultation is required with the FBI—and who is the "other appropriate Federal entity" for consultation?
- Why does this requirement apply only to Chinese entities?

But § 516 does not include legislative history to guide either the agencies or contractors in how to comply with its terms.

A number of industry trade groups have combined to oppose the restrictions in § 516 as being unworkable. See, e.g., BSA/The Software Alliance et al., Letter to Congressional Leadership (April 4, 2013), available at *www.bsa.org*. If § 516 remains unchanged, these agencies and contractors will face major challenges in acquiring IT systems due to the difficulties in determining whether such systems include Chinese-derived components and assessing whether any "risk of cyber-espionage or sabotage" may exist.

Security Rules for the Health Care Industry: Although not new, the Health Insurance Portability and Accountability Act (HIPAA) required implementation of security standards for health information, including

"reasonable and appropriate administrative, technical, and physical safeguards" to ensure the integrity and confidentiality of such information, protect against "reasonably anticipated" threats and unauthorized uses and disclosures, and otherwise ensure compliance. 42 USCA § 1320d-2(d). Years ago, HHS issued regulations incorporating cybersecurity requirements for "protected health information" (PHI).

On January 25, HHS published new HIPAA regulations making major changes in how the public and private sectors must protect PHI. 78 Fed. Reg. 5566 (2013). Key revisions include subjecting additional entities to cybersecurity requirements (security rule), imposing liability directly upon business associates and downstream subcontractors, and presumptively requiring breach notification in more situations. Some of the key changes include the following.

Breach Notification. Under the prior rule, covered entities had greater flexibility in determining whether breach notification would be required, as HHS only required notification if there was a "*significant* risk of financial, reputational, or other harm to the individual." In the final rule, HHS eliminated the more subjective "risk of harm" standard that previously applied when determining whether a security incident constituted a "breach" requiring individual notification.

The final rule establishes a presumption that any impermissible use or disclosure of PHI constitutes a breach that compromises the security or privacy of the information. The covered entity or business associate bears the burden of proving a low probability that the PHI has been "compromised," thus avoiding the need to notify. HHS characterized the previous "risk of harm" standard as too subjective, undermining uniformity regarding the duty for notification. Thus, the new risk assessment standard focuses on whether unauthorized recipients have accessed or had the opportunity to access PHI, rather than the risk of harm to an individual.

Penalty Methodology and Assessment. In the final rule, HHS also raised the stakes for violations and data breaches by widening its enforcement net and invoking tougher penalties. HHS finalized the increased liability structure created by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of P.L. 111-5, Act by: (1) applying civil monetary penalties to violations of the HITECH Act and implementing regulations, (2) subjecting business associates and all downstream subcontractors to direct liability for certain HIPAA violations (discussed below), and (3) increasing the monetary penalties for such violations. The degree of culpability determines the range of the potential penalty for each violation of a given provision, as illustrated by the following table.

TABLE 2—CATEGORIES OF VIOLATIONS AND RESPECTIVE PENALTY AMOUNTS AVAILABLE

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

The precise fine will depend on factors set forth in 45 CFR § 160.408, such as the nature and extent of the violation (including the number of persons affected and time period during which the violation occurred), the nature and extent of the resulting harm, the history of prior compliance with the provision, the financial condition of the covered entity or business associate, and "such other matters as justice may require." The final rule also clarified how HHS will impose fines for "multiple identical violations" where the violation of a provision affects multiple people or is ongoing. In such cases, HHS may impose a separate fine for each person affected by a violation or for each day that the violation continued.

Business Associate Direct Liability. Under the prior rule, the HIPAA obligations applied directly to covered entities, but business associates generally faced only contractual liability to the covered entity depending on what had been flowed down by the covered entity. The final rule makes business associates and their subcontractors directly liable for violating the HIPAA security rule, as well as certain provisions of the privacy and breach notification rules. These provisions include:

- impermissible uses and disclosures;
- failure to provide breach notification to the covered entity;

- failure to provide access to a copy of electronic PHI to either the covered entity, the individual or the individual's designee (whichever is specified in the business associate agreement);
- failure to make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request;
- failure to enter into business associate agreements with subcontractors that create or receive PHI on their behalf;
- failure to disclose PHI where required by the secretary to investigate or determine the business associate's compliance with the HIPAA rules;
- failure to provide an accounting of disclosures (if subject to those requirements pursuant to the business associate agreement); and
- failure to comply with the requirements of the security rule.

The final rule also establishes a parallel set of contractual requirements for subcontractors of business associates who create, receive, maintain or transmit PHI on behalf of the business associate. In the final rule, covered entities must obtain satisfactory assurances regarding the protection of PHI from their business associates, and business associates must do the same with their subcontractors, and so on, no matter how far "down the chain" the information flows.

Business Associate "Conduit" Exception. The HIPAA regulations previously carved out an exception to the definition of "business associate" for entities that serve merely as "conduits" through which PHI travels (such as the U.S. Postal Service). Many data storage companies had sought to expand this exception in the final rule to cover arrangements in which an entity stores, but does not normally access, PHI that it maintains on behalf of a covered entity. However, the final rule rejected attempts to exempt more entities from HIPAA compliance.

Instead, business associates now include a wide array of entities, such as: (1) health information organizations, E-prescribing gateways, or other persons that provide data transmission services involving PHI to a covered entity and that require routine access to such PHI; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity (i.e., a personal health record vendor). Although the final rule does not provide a bright-line test for what constitutes "routine access," the rule does clarify that the conduit exception is intended to exclude only those entities providing courier services, such as the Postal Service or United Parcel Service, and their electronic data transmission equivalents, such as internet service providers.

Security Standards for Critical Infrastructure Sectors: As discussed above, President Obama issued EO 13636, "Improving Critical Infrastructure Cybersecurity," in February. This latest executive order builds on prior statutory authority under the Homeland Security Act of 2002, tasking the Department of Homeland Security to "develop a comprehensive national plan for securing key resources and critical infrastructure of the United States," including IT. 6 USCA § 121(d)(5).

EO 13636 calls for a "baseline framework" for reducing cyber risk to the various critical infrastructure sectors:

> Sec. 7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure. (a) The Secretary of Commerce shall direct the Director of the National Institute of Standards and Technology (the "Director") to lead the development of a framework to reduce cyber risks to critical infrastructure (the "Cybersecurity Framework"). The Cybersecurity Framework shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act, as amended (15 U.S.C. 271 et seq.), the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113), and [Office of Management and Budget] Circular A-119, as revised.

78 Fed. Reg. 11740–41. In short, this executive order seeks to bring a degree of uniformity—along with minimum standards—to the various sectors of critical infrastructure.

However, the drafters of the cybersecurity framework will not be writing on a blank slate. To the contrary, many critical infrastructure sectors have already been tasked with addressing cyber-

security standards. 2007 Homeland Security Appropriations Act, P.L. 109-295, § 550; 6 CFR §§ 27.215, 27.225, 27.230, 27.235, 27.240, 27.245 (chemical sector); Electricity Modernization Act (title XII), P.L. 109-58, § 1211, 119 Stat. 941–42 (2005); 7 CFR §§ 1730.20, 1730.21, 1730.22, 1730.27, 1730.28 (energy sector); 10 CFR § 73.1 (nuclear sector); 9/11 Act, P.L. 110-53, § 1512(d) (railroad and bus carriers).

For sectors and industries that have already invested in cybersecurity defenses built to existing statutory and regulatory standards, the predictable reaction will be to avoid material changes imposing significant rework and additional cost. Thus, the existing patchwork of critical infrastructure cybersecurity standards may serve as a countervailing factor weighing against new cyber standards emerging from the executive order's cybersecurity framework, particularly for these sectors that have already implemented sector-specific standards.

EO 13636 also requires DOD and GSA to work with the Federal Acquisition Regulatory Council and prepare a report addressing "what steps can be taken to harmonize and make consistent procurement requirements related to cybersecurity." 78 Fed. Reg. 11742 (2013). In an RFI, the Joint Working Group on Improving Cybersecurity and Resilience Through Acquisition has sought information "about any conflicts in statutes, regulations, policies, practices, contractual terms and conditions, or acquisition processes affecting federal acquisition." 78 Fed. Reg. 27968 (2013). In performing this overview of the federal acquisition process, the joint working group will find a patchwork of agency-specific regulations with both major and minor differences in cybersecurity requirements and standards. See, e.g., Defense Federal Acquisition Regulation Supplement § 239.7102-1; GSA Acquisition Manual (GSAM) § 539.700; Department of Homeland Security (HSAR) § 3004.470; Health and Human Services Acquisition Regulation subpt. 339.71; NASA FAR Supplement § 1804.470-1.

Of greater concern, many agencies incorporate internal instructions and policies into the acquisition process, introducing even greater variation and uncertainty regarding federal cybersecurity standards. See, e.g., DFARS § 239.7102-1 (various DOD directives and policies); GSAM § 539.7001(d) (GSA CIO IT Security Procedural Guide); HSAR § 3004.470-2 (various DHS directives and policies). To the extent that such internal guidance has not been published for public notice and comment, this guidance not only impedes the executive order's directive to harmonize cybersecurity standards and practices, but also raises questions about compliance with the Administrative Procedure Act. 5 USCA § 552(a); see also *NI Indus., Inc. v. U.S.*, 841 F.2d 1104, 1107 (Fed. Cir. 1988) (declining to enforce internal agency procedures that had not been previously published in the *Federal Register*); 30 GC ¶ 119.

Conclusion—In summary, cybersecurity law and policy have not been static in the past 18 months. While the latest executive order seeks to move cyber standards towards a common framework, the absence of comprehensive cyber legislation has allowed the march towards sector-specific regulation and cyber safeguards to continue without a break in stride. For companies crossing several industries and critical infrastructure sectors, the path towards more robust cybersecurity programs and procedures will be increasingly uneven, as different types of data in separate sectors will trigger sector-specific requirements, thus further complicating the already difficult efforts to build corporate-wide, cost-effective cyber defenses.

✦

This Feature Comment was written for The Government Contractor by* David Z. Bodenheimer, *a partner, and* Elliot R. Golding, *an associate, in Crowell & Moring LLP's Washington, D.C. office. Mr. Bodenheimer specializes in Government Contracts and heads the Homeland Security practice. He currently serves as chair of the ABA Science & Technology Law Section's Security, Privacy, and Information Law Division and co-chair of the Public Contract Law Section's Cybersecurity, Privacy, and Data Protection Committee. Mr. Golding specializes in Privacy & Cybersecurity compliance counseling and security incident litigation regarding a wide range of laws and regulations, such as: HIPAA and HITECH; GLBA; state laws regarding pre-breach security requirements, breach notification, and unfair/deceptive trade practices; and foreign laws governing data privacy and security.

