Bloomberg BNA Federal Contracts Report™

Source: Federal Contracts Report: News Archive > 2014 > 03/25/2014 > BNA Insights > Cybersecurity: Cybersecurity Requirements for Government Contractors: Untangling the Web

**101 FCR 336**

***Cybersecurity***

# Cybersecurity Requirements for Government Contractors: Untangling the Web




**By Elizabeth A. Ferrell, Phillip R. Seckman, Erin B. Sheppard, Michael J. McGuinn**

*Elizabeth Ferrell (eferrell@mckennalong.com) and Phillip R. Seckman (pseckman@mckennalong.com), are partners in McKenna Long & Aldridge LLP's government contracts practice. Erin B. Sheppard (esheppard@mckennalong.com), and Michael J. McGuinn (mmcguinn@mckennalong.com) are associates in the firm's government contracts practice.*

Whether contractors are ready or not, broad-based cybersecurity regulations are on the way. The past three years have witnessed repeated disruption to the existing cybersecurity landscape from presidential, congressional, and agency-level action. Contractors face a dizzying maze of potential new cybersecurity requirements, overlaid upon an existing patchwork of often difficult-to-reconcile and varied regulations.

Companies operating in a slumping contracting environment of increased competition and ever-tighter purse strings cannot afford to ignore these developments. The potential consequences of noncompliance are significant, ranging from negative past performance evaluations and ineligibility to more severe consequences, including terminations for default, suspension or debarment, or False Claims Act liability. Data breaches are front-page fodder and reputational damage is often exorbitant. And all the while, the attacks continue, increasing in number and sophistication.

Over the next several months, attorneys from McKenna Long & Aldridge will write a series of articles for *Federal Contracts Report* to help guide contractors through the complex and evolving web of cybersecurity requirements. Addressing issues for contractors throughout the supply chain, both large and small, these articles will delve into the recent spate of cybersecurity developments, apprising contractors of new developments as they arise. The series will provide guidance on the implementation of broadly applicable security standards, like the National Institute for Standards and Technology's (NIST) recently-issued Cybersecurity Framework, as well as agency-specific security standards. We will also address breach reporting requirements applicable to government contractors. By the end of this series, contractors should be better equipped for the coming reality of cybersecurity compliance requirements.

## 1. Surveying the Landscape

Over the last three years, the government has dramatically expanded potential cybersecurity requirements applicable to government contractors. Significant developments include: (a) the proposed FAR rule on safeguarding contractor information systems; (b) the final DFARS rule on unclassified controlled technical information; (c) the president's executive order on critical infrastructure cybersecurity; (d) the NIST Cybersecurity Framework; (e) the GSA/DoD report on the use of cybersecurity in acquisition planning and contract administration; and (f) several congressional initiatives in the cyber arena. We provide a basic summary of these developments below.

### a. The Proposed FAR Rule on Safeguarding Contractor Information Systems

On August 24, 2012, the FAR Councils issued a proposed rule requiring contractors to safeguard contractor information systems containing information provided by or generated for the government. *See* 77 Fed. Reg. 51496 (Aug. 24, 2012). The proposed rule would add a new FAR subpart and contract clause to make basic information protection measures a contract requirement. It would apply broadly to any prime contractor and subcontractor information systems containing information "provided by or generated for the government (other than public information)."

The proposed rule, if implemented, would impose specific safeguarding requirements for contractor information systems. Contractors would be subject to requirements pertaining to: (1) public computers and web sites; (2) transmitting electronic information; (3) voice and fax transmissions; (4) physical and electronic barriers; (5) sanitization; (6) intrusion protection; and (7) subcontract transfers. The requirements are intended to serve as the

baseline of security standards applicable to government contractors, effectively establishing the lowest common denominator of cybersecurity requirements.

As of this writing, the proposed rule still has not been issued. [1] And given subsequent developments discussed in this article, most significantly the GSA/DoD report, the proposed rule may never be issued, at least not in its current form.

[1] The original due date for a draft final rule was December 2012; however, that due date has been extended multiple times. The current deadline is April 2, 2014. *See* DoD AT&L Open FAR Cases, available at www.acq.osd.mil/dpap/dars/opencases/**far**casenum/**far.pdf.**

**b. The Final DFARS Rule on Unclassified Controlled Technical Information**

On November 18, 2013, DoD issued a final DFARS rule imposing heightened security safeguards and mandatory reporting requirements on all DoD prime contractors and subcontractors handling unclassified controlled technical information (UCTI). 78 Fed. Reg. 69273 (Nov. 18, 2013). The rule defines UCTI as technical data or computer software with military or space application, subject to controls on access, use, disclosure or distribution, and marked in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents.

For contractors handling UCTI, the DFARS rule imposes two requirements: (1) safeguarding information systems containing any unclassified controlled technical information; and (2) reporting and investigation of cyber incidents. First, the rule requires contractors handling UCTI to comply with 51 security controls from NIST's Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Contractors lacking, or opting not to implement, a certain control must be able to explain why that control is inapplicable or that an alternative control achieves the same protection. Contractors also must implement additional security controls if they have information that additional security is needed based on "an assessed risk or vulnerability."

Second, the DFARS rule requires covered contractors to report "cyber incidents" within 72 hours of discovery. The rule defines cyber incidents broadly and requires contractors to report up to 13 categories of information to DoD. Prime contractors also must report incidents on behalf of subcontractors. After the 72-hour report, covered contractors must conduct a comprehensive review of the incident, and DoD also may elect to conduct its own damage assessment into the incident.

The new clause, DFARS 252.204-7012, effective November 18, 2013, is now being included in DoD solicitations and contracts. Impacted contractors must immediately determine where UCTI is located on contractor and subcontractor information systems. Contractors with UCTI need to map their system compliance against the rule's security standards, or be prepared to explain why particular standards do not apply or why other protections provide adequate security. Contractors should investigate possible system compromises of UCTI immediately and thoroughly. Contractors also should implement policies to ensure internal compliance with the DFARS requirements, and contractors should modify subcontract terms and conditions as necessary to ensure that subcontractors' compliance. Finally, in crafting such policies and the strategy for compliance, contractors should be mindful of the risks that forensic or other government investigations of computer systems and data present to their business and competition-sensitive as well as privileged information.

**c. The President's Executive Order 13636**

In addition to the foregoing regulatory developments, President Obama on February 12, 2013 signed Executive Order (EO) 13636 to enhance protections of the nation's critical infrastructure from cyber attacks. The EO's purpose was to improve cybersecurity of the nation's "critical infrastructure," defined as systems whose incapacity or destruction would result in a debilitating impact on national security, the economy, or public health and safety. Critical infrastructure includes, among other sectors, the Defense Industrial Base, Critical Manufacturing, Energy, and Information Technology.

Most significantly here, the EO required that: (1) NIST work with stakeholders to develop a voluntary framework – based on existing standards and best practices – for reducing cyber risks to critical infrastructure; and (2) DoD and GSA make recommendations to the president regarding "the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration." As discussed below, NIST and DoD/GSA have each responded to the EO.

**d. The NIST Cybersecurity Framework**

Acting on the EO directive, NIST last month issued Version 1.0 of the Cybersecurity Framework. The Framework is a voluntary, living document that captures and organizes current best practices for use by critical infrastructure providers implementing voluntary cybersecurity programs. The Framework links a set of key cybersecurity concepts to desired outcomes and provides a range of standards, guidelines, metrics, and other resources for entities to utilize in attaining those outcomes. The Framework also provides a rubric for differentiating between the varying levels of rigor and sophistication present in various organizations' cybersecurity plans.

Though developed for providers of critical infrastructure services, the processes, procedures, and organizational constructs identified in the Framework are useful to any entity seeking to assess its cybersecurity risks. It also warrants careful consideration for a number of reasons. First, if widely adopted by critical infrastructure entities, the Framework may become the de facto standard of care for companies seeking to protect their own assets from cyber risks. Second, the Framework provides an easily accessible organizational construct for discussing the

components of such a plan with internal and external stakeholders. Finally, the Framework may also serve a model for future legislative and regulatory requirements that extend beyond critical infrastructure industries.

How companies proceed in light of the voluntary nature of the Framework will be highly individualized. Moreover, given the flexible nature of the Framework, the precise definition of "implementation" of the Framework also will vary almost entirely by entity. Regardless of where an individual company may fall on this spectrum, all organizations should continue to monitor developments in this area as the substance and voluntary nature of the Framework continue to evolve.

**e. The GSA/DoD Joint Working Group Report on Improving Cybersecurity and Resilience Through Acquisition**

Responding to Section 8(e) of the EO, the DoD and GSA Joint Working Group submitted its final report to the president on January 23, 2014, titled *Improving Cybersecurity and Resilience Through Acquisition.* The Joint Working Group's final report makes six recommendations concerning the use of cybersecurity standards in federal acquisitions:

- Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions.
- Address cybersecurity in relevant training
- Develop common cybersecurity definitions for federal acquisitions
- Institute a federal acquisition cyber risk management strategy
- Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other "trusted" sources, whenever available, in appropriate acquisitions
- Increase government accountability for cyber risk management

The Joint Working Group's recommendations show that federal contractors will soon be subject to significant cybersecurity compliance obligations. At the same time, however, the report contains a number of ambiguities. Most notably, it does not specify what changes to existing procurement regulations are needed in order to incorporate new security standards and compliance requirements. This includes, for example, how the report's recommendations will align with the proposed FAR rule and the final DFARS rule discussed above. The report also fails to meaningfully explain the consequences of a contractor's noncompliance with applicable standards.

GSA and DoD recently issued a notice for public comment on a draft implementation plan and appendix related to their recommendations. 79 Fed. Reg. 14042 (Mar. 12, 2014). According to this release, GSA and DoD intend to first implement the recommendation to institute a federal acquisition cyber risk management strategy. As part of this process, GSA and DoD will be categorizing procurements based on comparative cyber risk, and they are seeking stakeholder input on the implementation process. This process will also involve the creation and use of security "overlays" to address various cyber risks depending on the risk profile of particular acquisitions. Contractors and industry organizations should closely follow and participate in the GSA and DoD implementation process.

**f. Congressional Action**

Not to be left out, Congress also has gotten in on the cybersecurity action, though certainly not to the degree that some had hoped. In fact, many of the perturbations in the cybersecurity landscape in the past year, beginning with E.O. 13636, were prompted by the absence of comprehensive legislation from Congress. What has arisen from Congress, however, are a handful of important developments, two of which we briefly discuss below, the balance of which will be addressed in a future article.

Section 941 of the FY 2013 National Defense Authorization Act ("NDAA") requires "cleared defense contractors" to provide "rapid reporting" of successful penetration of contractor networks. "Cleared defense contractors" are private entities with clearance to access, receive or store classified information in support of DoD programs. In addition to rapid reporting, Section 941 mandates that cleared defense contractors are to provide DoD with access to contractor systems upon request. Although Section 941 requires that DoD promulgate implementing regulations within 90 days, DFARS Case No. 2013-D018 has yet to result in the issuance of a rule. [2] Eventually, the rule likely will define what "rapid reporting" means and in particular what information must be reported, the level of DoD access to contractor systems to investigate the incident, and clarify the degree to which the reporting requirement extends to a cleared defense contractor's unclassified networks.

[2] A report on the draft rule was due March 19, 2014. *See* DoD AT&L, Open DFARS cases, available at www.acq.osd.mil/dpap/dars/opencases/**dfars**casenum/**dfars**.pdf.

Another important legislative development for cybersecurity involves Section 818 of the FY 2012 NDAA, relating to counterfeit parts. While this section of the FY 2012 NDAA specifically addresses the detection and avoidance of counterfeit electronic parts in the DoD supply chain, there is an important nexus between counterfeit parts and

cybersecurity. In addition to the pressing reliability issues of counterfeit parts, vulnerabilities and back doors in counterfeit information and communications technology components (e.g., hardware, firmware) increase the risk of future cyber attacks. The GSA/DoD Joint Working Group report discussed above reiterates this nexus in its recommendations, stating that contractors should purchase from original equipment manufacturers, their authorized resellers, or other "trusted" sources, whenever available, in certain higher-risk acquisitions. Contractors should expect this focus on trusted parts and suppliers to become a key component of cybersecurity compliance.

**2. What's Next**

Over the next few months, McKenna's article series will provide an in-depth discussion of these developments and relevant cybersecurity requirements.

---



ISSN 1523-5696