THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 59, No. 4 **February 1, 2017**

Focus

¶ 25

FEATURE COMMENT: Achieving Cyber-Fitness In 2017: Part 1—Planning For Compliance

It is a new year, which means New Year's resolutions for roughly 50 percent of Americans. Most vow to lose weight or save more money. For many Government contractors, however, the focus in 2017 is cybersecurity in general, and specifically compliance with the Department of Defense's final rule for safeguarding covered defense information before the December 31 deadline. See 81 Fed. Reg. 72986 (effective Oct. 21, 2016).

Under Defense Federal Acquisition Regulation Supplement 252.204-7012, defense contractors that process, store or transmit "covered defense information" (CDI) must meet more than 100 security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

Although the deadline is nearly a year away, compliance cannot be achieved overnight, or even in a few months for that matter. To put this in perspective, experts estimate a defense contractor with 600 employees should anticipate that a third-party compliance audit of its information systems and data will take three to six months, and this does not include the time needed to correct any deficiencies identified during the audit.

Although the DFARS rule is the primary cybersecurity concern for many contractors, they may need to address other cybersecurity rules in 2017, depending on the specific contracts and the types of information with which a contractor deals. For example, a contractor selling medical devices to the Department of Veterans Affairs may fall under different safeguarding and reporting requirements than a contractor providing cloud services for an educational agency or a state university. The former scenario likely implicates health-care data, which is heavily regulated at both the federal and state level; the latter scenario could implicate the privacy protections for children under the Children's Online Privacy Protection Act, or students' personally identifiable information under the Family Educational Rights and Privacy Act. In both cases, a contractor might have to answer to more than one enforcement agency for compliance failures. Thus, navigating the labyrinth of regulations can be overwhelming, and a wrong step may result in severe consequences, including termination or, potentially, False Claims Act allegations.

Preparing, implementing and maintaining a comprehensive cybersecurity plan that identifies and tracks the location of contractor systems and data is key to preventing undesirable consequences. Contractors that become familiar with the applicable cybersecurity requirements, develop a robust cybersecurity program, and regularly exercise and test their cybersecurity controls are better positioned to take advantage of safe harbor provisions and avoid common compliance pitfalls.

This Feature Comment is the first in a multi-part series dedicated to Government contractor "cyber-fitness." The series will focus on the DFARS and FAR cybersecurity requirements (as well as other cybersecurity regulations and standards that may apply to Government contractors), providing guidance and insight to assist contractors in understanding the regulations and developing a path to compliance by December 31. In addition to parsing the regulations, articles in this series will explore the systems and data covered by the regulations; the role of third-party auditors in achieving and maintaining compliance; cybersecurity considerations when negotiating subcontracts, teaming agreements and joint ventures; reporting requirements; and developing an effective cyber-incident response plan. Most importantly, this series is intended

to serve as a practical tool for contractors by not only demystifying the regulations, but also by highlighting best practices gathered from discussions with security audit experts and Government insiders.

DFARS and FAR Requirements for Safeguarding Information—As noted above, DOD contractors are to implement NIST SP 800-171, which includes 14 "families" of security controls, no later than December 31. However, they are encouraged to achieve compliance "as soon as practical." DFARS 252.204-7012.

Early assessment and compliance is advisable, as agencies increasingly will focus on cybersecurity in issuing solicitations and awards. As of now, contractors must provide the DOD chief information officer with "a list of the security requirements that the contractor is not implementing at the time of award" within 30 days after contact award. DFARS 252.204-7012. A contractor that can demonstrate compliance before the end of the year may have an advantage, particularly because the final rule "does not preclude a requiring activity from specifically stating in the solicitation that compliance with the NIST SP 800-171 will be used as an evaluation factor in the source se[le]ction process." 81 Fed. Reg. 72990. Thus, contractor cyber-fitness may be key to award decisions made in the near future.

It is generally advisable to start any analysis at the beginning, so here is a review of the basic definitional constructs that govern under the regulations.

DFARS: The DOD regulations require that contractors provide "adequate security on all *covered contractor information systems*." DFARS 252.204-7012(b) (cloud computing service providers have their own security requirements at DFARS 252.239-7010). Covered contractor information systems are defined by the fact that they house or touch "covered defense information." DFARS 252.204-7012(a) (" 'Covered contractor information system' means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.").

Prior to implementation of the final DFARS rule, the Government received comments seeking clarification on the definition of CDI, with several contractors hoping this information could be limited to that specifically designated by the Government under a contract. The drafters of the final rule acknowledged the "affirmative requirement for Government to mark or otherwise identify in the contract all covered defense information ... while recognizing the shared obligation of the contractor to recognize and protect covered defense information that the contractor is developing during contract performance." 81 Fed. Reg. 72988. Thus, although contractors may rely on their customer to identify CDI, they also must remain vigilant and proactive when it comes to safeguarding CDI.

The definition of CDI in the final rule reads:

> *Covered defense information* means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, and is—
>
> (1) Marked or otherwise identified in the contract, task order or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
>
> (2) Collected, developed, received, transmitted, used or stored by or on behalf of the contractor in support of the performance of the contract.

DFARS 252.204-7009 (81 Fed. Reg. 72998).

The definition is broad, and its two-part test leaves considerable room for confusion, disagreement and recrimination. Part 1 of this test refers the contractor to the existing CUI Registry. However, the CUI Registry is rather generic and provides little guidance with respect to specific documents.

This problem is mooted if the first alternative for part 2 of the test—i.e., customer markings—is satisfied. Those markings put the contractor on notice with respect to the status of the information. Absent those markings, however, the contractor is left with the generic CUI Registry descriptions, which the contractor must then evaluate against all information "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." Thus, while contractors would be wise to conduct a thorough company-wide review of their data and systems at the outset, focusing on their DOD contract materials to identify and segregate all systems that may house or share CDI, there is ample room for uncertainty about which information is CDI. Contractors will likely err on the side of caution; if not, it would be prudent to document contemporaneously the rationale for treating information as other than CDI.

FAR: Under the FAR, contractors must protect information systems that process, store or transmit "*Federal contract information*" (FCI). FAR 52.204-21(b)(1). FCI is

> information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public websites) or simple transactional information, such as necessary to process payments.

Id.

This definition is extraordinarily broad. It includes any information used in the performance of a contract that originated from or will be provided to the Government, apart from information that is public or is "simple transactional information." Contractors should ensure that any system that stores or shares FCI is identified and adequate security controls are in place.

These systems are subject to 15 standards—relating to six of the 14 security control families in NIST SP 800-171. See FAR 52.204-21(b)(1)(i)–(xv); NIST SP 800-171 at 9–14. The rule relating to safeguarding systems with FCI has been in process for more than four years. So presumably contractors with FCI already have taken steps to implement security controls in accordance with the FAR, which should make compliance with all NIST SP 800-171 security controls under the DFARS regulations less onerous.

NIST SP 800-171: NIST SP 800-171 addresses requirements for properly protecting CUI, which includes CDI, on nonfederal information systems. NIST SP 800-171 contains more than 100 security requirements, of which 30 are "basic" requirements and 79 are "derived" requirements. It is based on the following security requirements that were implemented to protect federal information and information systems:

- Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems; and
- NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

The "basic" requirements in NIST SP 800-171, summarized below, originated from FIPS 200, which includes "high-level and fundamental security requirements for federal information and information systems," while the "derived" requirements are based on the security controls in NIST SP 800-53. See NIST SP 800-171 at 6. Although there are similarities between NIST SP 800-171 and NIST SP 800-53, NIST SP 800-171 is tailored to nonfederal contractor systems and does not include NIST SP 800-53's uniquely federal controls.

Fourteen Families of Security Requirements: The security requirements in NIST SP 800-171 are grouped into 14 families. Under the DFARS final rule, defense contractors must comply with the requirements in *each* of the 14 families delineated below. Under the FAR, contractors must safeguard FCI based on six of the families. See Table 1 below. The families identified with a star (*) below are likely to be the most time-consuming for contractors to implement and may pose the most risk if not thoroughly addressed.

DFARS Requirements:

1. **Access Control**: Information system access, including permissions to conduct transactions, must be limited to *authorized* users. [Requirements: two basic, 20 derived.] Contractors housing FCI under FAR 52.204-21 are subject to two basic requirements and two derived requirements in this family. See Table 1 below.
2. ***Awareness and Training**: Managers and users must be made aware of the security risks associated with their activities (e.g., bypassing the network firewall). Personnel must be trained on their respective information security-related duties and responsibilities (e.g., reporting an insider threat). [Requirements: two basic, one derived.]
    - *Practitioner's Note*: Make no mistake, awareness and training controls can be time-consuming to implement and maintain—employees require initial training and periodic refresher training; training requirements vary depending on roles and responsibilities; and training programs must mature in a manner consistent with technology and the cyber-threat environment. Organizations with comprehensive training programs are best situated to mitigate exposure in the event of a breach. This is because data breaches resulting from human factors can cause massive damage—regardless of whether the cause is intentional or malicious. Most

organizations are cognizant of the threat posed by malicious insiders, but the more persistent threat is *non*-malicious employee actions. Have you ever sent a document to your personal e-mail account because your company's virtual private network was too slow? Did you later download the document onto your work computer? If so, you represent the majority of employees—90 percent to be exact—who violate their organization's information security safeguards. Although seemingly innocent, nearly *half* of all internal cybersecurity failures are attributed to this type of behavior. See SC Magazine UK – News, Nov. 2, 2016, available at *https://www.scmagazineuk.com/90-of-employees-violate-data-breach-prevention-policies/article/570413/*. Unsurprisingly, security executives view human behavior as their greatest vulnerability. (The Nuix, 2016 Defending Data Report finds that 97 percent of security executives agreed that human behavior was their greatest vulnerability.) Understanding this reality and building a robust training program are important steps in achieving true cyber-fitness.

3. **Audit and Accountability**: Information system audit records must be created and retained to enable the monitoring, analysis, investigation and reporting of unlawful, unauthorized or inappropriate activity. Additionally, contractors must trace user activity to hold individuals accountable for violating system security policies. [Requirements: two basic, seven derived.]
4. **Configuration Management**: Baseline configurations and inventories of organizational information systems (including hardware, software, firmware and documentation) must be maintained. Security configuration settings for information technology products employed in organizational information systems must be established and enforced. [Requirements: two basic, seven derived.]
5. **Identification and Authentication**: Contractors must identify information system users, processes acting on behalf of users or devices, and authenticate the identities of those users, processes and devices as a prerequisite for access to information systems. [Requirements: two basic, nine derived.] Contractors housing FCI under FAR 52.204-21 are subject to two basic requirements in this family. See Table 1 below.
6. **Incident Response**: Contractors must establish an operational incident-handling capability for their systems that includes adequate preparation, detection, analysis, containment, recovery and user response activities. They also must establish a procedure for documenting and reporting incidents to appropriate officials or authorities. [Requirements: two basic, one derived.]
7. **Maintenance**: Contractors must perform maintenance on their systems and provide effective controls on the tools, techniques, mechanisms and personnel used to conduct maintenance. [Requirements: two basic, four derived.]
8. **Media Protection**: Contractors must protect information system media, both paper and digital, and limit access to media. Such media must be sanitized or destroyed before disposal or release for reuse. [Requirements: three basic, six derived.] Contractors housing FCI under FAR 52.204-21 are subject to one basic requirement in this family. See Table 1 below.
    - *Practitioner's Note*: Proper disposal of information may implicate privacy statutes or other federal requirements, depending on the data. For example, the "Disposal Rule," promulgated in 2005 under the Fair and Accurate Credit Transactions Act, requires any company collecting consumer information for a business purpose to dispose of that information in a way that prevents unauthorized access and misuse of the data. See 16 CFR § 682.
9. **Personnel Security**: Contractors must screen individuals (including third-party service providers) before they are given access to information systems. Data must be protected during and after personnel actions such as terminations and transfers. [Requirements: two basic, zero derived.]
10. ***Physical Protection**: Contractors must limit physical access to information systems, equipment and the respective operating environments to authorized individuals, as well as protect and monitor physical facilities and

support infrastructure for information systems. [Requirements: two basic, four derived.] Contractors housing FCI under FAR 52.204-21 are subject to one basic requirement and one derived requirement in this family. See Table 1 below.

- *Practitioner's Note*: Microsoft offers a simple, albeit brutal, statement on the significance of physical security: "*Without physical security, no other security measures can be considered effective.*" See Tom Caddy, Physical Security 101, NIST CMVP Physical Security Conference at 3 (Sept. 15, 2005). Assuming this is correct, contractors who have spared no expense to implement state-of-the-art technology controls, but whose employees work from multiple geographic locations, are at an inherent disadvantage for enforcing safeguards for CUI under this control. Thus, this family of requirements may pose greater challenges to contractors that have employees in multiple locations than to others with employees working exclusively on-site with DOD.

11. **Risk Assessment**: Contractors must periodically assess the risk to organizational operations (including mission, functions, image or reputation), organizational assets and individuals resulting from the operation of organizational information systems and the associated processing, storage or transmission of organizational information. [Requirements: one basic, two derived.]
12. ***Security Assessment**: Contractors must periodically assess and monitor security controls for effectiveness, as well as implement plans to correct deficiencies and reduce or eliminate vulnerabilities. [Requirements: three basic, zero derived.]
    - *Practitioner's Note*: Technology used for security often is not the problem, rather it is the human element. For example, a new virus protection software or firewall patch may be released, but only a privileged user, i.e., the system administrator, can implement the update across the network. Security assessments also pose problems because there may be a judgment bias when an organization assesses its own system vulnerabilities or controls. Third-party audits most objectively and accurately assess security, but IT and security teams may dislike third parties peeking behind the curtain and critiquing their work. Although contractors do not want to wait to be hacked to find out the effectiveness of their security controls (or lack thereof), they can get stuck between an archetypal rock and a hard place if a begrudging IT team is unwilling to let in third-party auditors.
13. **System and Communications Protection**: Contractors must monitor, control and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. They must employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. [Requirements: two basic, 14 derived.] Contractors housing FCI under FAR 52.204-21 are subject to one basic requirement and one derived requirement in this family. See Table 1 below.
14. **System and Information Integrity**: Contractors must identify, report and correct flaws in a timely manner. Protection against malicious code must be in place at appropriate locations. Contractors must monitor information system security alerts and advisories, and take appropriate actions in response. [Requirements: three basic, four derived.] Contractors housing FCI under FAR 52.204-21 are subject to two basic requirements and two derived requirements in this family. See Table 1 below.

As mentioned above, the mandatory requirements for contractors processing, storing or collecting FCI under FAR 52.204-21, 15 in all, overlap with six of the control families in NIST SP 800-171. Table 1 below illustrates this overlap.

Roadmap to Compliance—The following guidelines are designed to assist contractors in complying with the DFARS safeguarding and reporting requirements by December 31. Contractors already implementing security controls in accordance with the FAR rule for FCI have a head start, but may consider conducting a company-wide review to bolster all

Table 1—NIST SP 800-171 and FAR 52.204-21			
NIST SP 800-171			**FAR 52.204-21**
	3.1	**ACCESS CONTROL**	
Basic	3.1.1	Limit information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems).	FAR 52.204-21(b)(1)(i)
Basic	3.1.2	Limit information system access to transactions and functions that authorized users are permitted to execute.	FAR 52.204-21(b)(1)(ii)
Derived	3.1.20	Verify and control connections to and use of external information systems.	FAR 52.204-21(b)(1)(iii)
Derived	3.1.22	Control information posted or processed on publicly accessible information systems.	FAR 52.204-21(b)(1)(iv)
	3.5	**IDENTIFICATION AND AUTHENTICATION**	
Basic	3.5.1	Identify information system users, processes acting on behalf of users, and devices.	FAR 52.204-21(b)(1)(v)
Basic	3.5.2	Authenticate the identities of those users, processes or devices as a prerequisite to allowing access to organizational information systems.	FAR 52.204-21(b)(1)(vi)
	3.8	**MEDIA PROTECTION**	
Basic	3.8.3	Sanitize or destroy information system media containing CUI before disposal or release for reuse.	FAR 52.204-21(b)(1)(vii)
	3.10	**PHYSICAL PROTECTION**	
Basic	3.10.1	Limit physical access to organizational information systems, equipment and the respective operating environments to authorized individuals.	FAR 52.204-21(b)(1)(viii)
Derived	3.10.3	Escort visitors and monitor visitor activity.	FAR 52.204-21(b)(1)(ix) (also, maintain audit logs of physical access; and control and manage physical access devices)

Table 1—NIST SP 800-171 and FAR 52.204-21			
NIST SP 800-171			FAR 52.204-21
	3.13	**SYSTEM AND COMMUNICATIONS PROTECTION**	
Basic	3.13.1	Monitor, control and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	FAR 52.204-21(b)(1)(x)
Derived	3.13.5	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	FAR 52.204-21(b)(1)(xi)
	3.14	**SYSTEM AND INFORMATION INTEGRITY**	
Basic	3.14.1	Identify, report and correct information and information system flaws in a timely manner.	FAR 52.204-21(b)(1)(xii)
Basic	3.14.2	Provide protection from malicious code at appropriate locations within organizational information systems.	FAR 52.204-21(b)(1)(xiii)
Derived	3.14.4	Update malicious code protection mechanisms when new releases are available.	FAR 52.204-21(b)(1)(xiv)
Derived	3.14.5	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened or executed.	FAR 52.204-21(b)(1)(xv)

security controls (if not done previously). Similarly, vigilant defense contractors that have tracked and implemented interim versions of the DFARS rule should be well equipped for compliance by the end of the year.

It should be noted that the drafters of the DFARS final rule hoped that NIST SP 800-171, which is tailored for contractor information systems, would "enable[] contractors to use systems they already have in place with some modification instead of building a new system." 81 Fed. Reg. 72997.

Although the following tips are not one-size-fits-all or a substitute for professional representation, you should consider the following when assessing your path to cyber-fitness in 2017.

Establish a Compliance Team: To start, contractors should identify an individual or team that will be responsible for cybersecurity compliance and accountable to management. The team should hold a kick-off meeting to (1) introduce team members, (2) assign roles and responsibilities, (3) discuss identified or perceived gaps, and (4) develop a plan and schedule for demonstrating compliance by December 31.

Data Mapping and Security Domains: Contractors should inventory and examine all of their systems and data. Third-party auditors recommend a data-focused approach rather than a systems approach because many contractor systems house multiple types of data. Additionally, contractors should think about how their systems are connected, i.e., which systems have access to data on other systems, even if the systems do not actively share data. While this may seem daunting, a thorough review at the beginning of the compliance process will allow for a complete solution and should minimize downstream issues resulting from certain systems being ignored in an assessment. Contractors may be able to isolate CDI or FCI—physically, logically or a hybrid of the two—into a specific security domain apart from other operations and assets, which would allow the contractor to avoid implementing strict security controls on all of its systems.

Schedule: Plan and schedule implementation activities after (1) conducting a gap analysis, (2) estimating how long it will take to address noncompliances, (3) identifying dependencies and (4) mapping the critical path. The timeline for implementing NIST SP 800-171 will be different for every organization depending on the size of the organization and the gaps. For example, awareness and training may not take long if the contractor already has a comprehensive training program. In contrast, this may be time-consuming for an organization that needs to implement training for several hundred employees who are geographically dispersed. Contractors should consider whether they will use a third-party auditor to achieve compliance. If so, the auditor's availability and timeline for completing the audit must be factored into the schedule. For example, it is estimated that auditing a domestic company with 600 employees and 30 servers generally takes between *three to six months*. Obviously, this time frame will change according to the number of employees and information systems that need to be audited. (*Note*: If your organization's cybersecurity health is uncertain, consider whether legal counsel will hire pre-audit auditors to assess your vulnerability, e.g., to ensure a hacker is not already accessing your system. Hiring the auditor through legal counsel should allow the initial assessment to remain privileged.)

Documentation: Track compliance in a matrix that aligns each NIST requirement with an explanation of how the company meets the requirement or plans to achieve compliance. This matrix may be initially drafted as part of the gap assessment, but it should be maintained and continuously updated as statuses change. It may be accessed later to determine the status of compliance and as evidence of compliance if questions arise.

Regular Reassessment: As noted above, cybersecurity and compliance must be viewed as ongoing processes involving periodic assessments of company data and systems. A written plan outlining regular actions to review and address cybersecurity issues is essential. Contractors should keep in mind that CDI includes information listed in the CUI Registry, which is subject to change. Thus, contractors should stay abreast of new information that may be classified as CUI, and thus falls within the safeguarding requirement. Further, new technology and receipt of additional contracts will affect the adequacy of contractor compliance.

Conclusion—Contractor cyber-fitness and timely compliance with DFARS regulations are certainly achievable with appropriate planning. Willingness to take a holistic approach to understanding systems and data subject to, or potentially subject to, cybersecurity requirements along with a comprehensive cybersecurity plan will enable contractor success this year and for many years to come.

✦

This Feature Comment was written for The Government Contractor by* John Chierichella, Townsend Bourne *and* Melinda Biancuzzo. *Mr. Chierichella is a partner in the Washington, D.C. office of Sheppard, Mullin, Richter & Hampton, a member of the firm's Government Contracts, Investigations, and Internal Trade practice group, and co-leader of the firm's Aerospace and Defense Industry team. Ms. Bourne and Ms. Biancuzzo are associates in Sheppard Mullin's Washington, D.C. office and members of the Government Contracts, Investigations, and Internal Trade practice group. They can be reached at jchierichella@sheppardmullin.com, tbourne@sheppardmullin.com and mbiancuzzo@sheppardmullin.com, respectively.