THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 59, No. 33 **September 13, 2017**

Focus

¶ 275

FEATURE COMMENT: Achieving Cyber-Fitness In 2017: Part 5—Cyber Incident Reporting And Response

As discussed in parts 1–4 of this series, the Defense Federal Acquisition Regulation Supplement cybersecurity clause, Safeguarding Covered Defense Information and Cyber Incident Reporting, mandates contractor compliance with the security controls in National Institute of Standards and Technology Special Publication (SP) 800-171 by December 31. DFARS 252.204-7012.

Thus far, we have focused on best practices for achieving compliance with the NIST security controls and other related laws and regulations, as well as considerations related to supplier and subcontractor compliance, to ensure proper safeguarding of covered defense information (CDI) and other data. This Feature Comment will focus on the second stated purpose of the DFARS cybersecurity clause—prescribing the reporting requirements for contractors that experience a cyber incident. (In this series, we have compared the DFARS requirements to those in the FAR provision for "basic safeguarding" of information systems. Note the FAR provision does *not* contain a discrete reporting requirement. FAR 52.204-21.)

Collecting information on cyber incidents is an important aspect of the Government's approach to monitoring and containing cyber threats. This is most obviously evidenced by the relatively recent execution of the Cybersecurity Information Sharing Act (CISA), which encourages voluntary disclosure of "cyber threat indicators" and "defensive measures" by private-sector organizations in exchange for certain protections. See P.L. 114-113.

Contractors should be aware of their obligations under the DFARS reporting requirements, including exactly when and what data must be shared with the Government, as well as collateral issues such as the consequences for a contractor and its data once the required information is shared with Uncle Sam. In this Feature Comment, we explore these issues, as well as practical considerations for a robust cyber incident response plan.

- *Note*: The Department Defense held an Industry Information Day on June 23, during which it provided a four-hour presentation outlining important cybersecurity regulations and information relating to broader cybersecurity concerns. DOD clarified that "compliance" with DFARS 252.204-7012 by December 31 will be viewed as contractor completion of (1) a system security plan (SSP) and (2) a plan of action and milestones (POA&M). This is a departure from previous readings of the provision, which interpreted "compliance" to mean demonstration of implementation of all NIST SP 800-171 security controls, or sufficient alternative controls. Although the clarification from DOD allows more leeway for contractors, DOD left open the possibility that failure to have the controls fully implemented could be considered in agency evaluation and source selection decisions, and thus could lead to negative source selection consequences for contractors that have not achieved full implementation by year end. Slides from the DOD industry day presentation are available at *dodcio.defense.gov/Portals/0/Documents/Public%20Meeting%20-%20Jun%2023%202017%20Final.pdf?ver=2017-06-25-022504-940*. A video from the industry day is available at *dodcio.defense.gov/IID/videoid/544122/#DVIDSVideoPlayer90061*.

The DFARS "Rapid Reporting" Requirement—DFARS 252.204-7012 includes a requirement that contractors must "rapidly" report cyber incidents to DOD. DFARS 252.204-7012(c). A "cyber

incident" is defined as "action[] taken through the use of computer networks that result[s] in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." DFARS 252.204-7012(a); see DOD Industry Day, slide 65 (June 23, 2017). The DFARS provision states,

> When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall—
>
> (i) *Conduct a review for evidence of compromise of covered defense information*, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and
>
> (ii) *Rapidly report cyber incidents to DoD* at http://dibnet.dod.mil.

DFARS 252.204-7012(c) (emphasis added).

"Compromise," as used in the DFARS provision, is defined as "disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred." DFARS 252.204-7012(a). Thus, contractors should monitor information systems and CDI for abnormal activity that may indicate the occurrence of a cyber incident. Contractors must review systems and hardware affected by a cyber incident to discern the extent of the CDI compromise, and must report the cyber incident to DOD. Per the regulation, " '[r]apidly report' means within 72 hours of discovery of any cyber incident." DFARS 252.204-7012(a).

A key issue that may become a source of contention between contractors and the Government is identifying when "discovery" occurs for purposes of triggering the 72-hour reporting requirement. A former Government insider to whom we spoke advocated the institutional use of a "confirmed incident," as defined by a clear organizational process, as an appropriate reporting "trigger." This approach would allow contractors to investigate anomalous activity as part of their normal monitoring processes, and prevent overloading DOD with reports of inconsequential issues. As discussed below, a defined cyber incident response plan with a clear process for assessing possible "confirmed incidents" would provide internal consistency and proof of a responsible process when dealing with possible critics of the timing of a contractor's reports.

Cyber Incident Reporting—To report a cyber incident, a contractor must have a DOD-approved medium assurance certificate. DFARS 252.204-7012(c)(3) (stating that information on obtaining a medium assurance certification is available at *http://iase.disa.mil/pki/eca/Pages/index.aspx*). A contractor's cyber incident report shall contain as many of the following elements as possible:

- company name and point of contact information;
- Data Universal Numbering System (DUNS) number;
- contract number(s) or other type of agreement affected or potentially affected;
- Contract or other type of agreement clearance level;
- Government program manager point of contact (address, position, telephone, e-mail);
- facility clearance level (unclassified, confidential, secret, top secret, not applicable);
- facility Commercial and Government entity code;
- incident location CAGE code;
- location(s) of compromise;
- date incident discovered;
- incident/compromise narrative;
- type of compromise (unauthorized access, unauthorized release, unknown, not applicable);
- description of technique or method used in cyber incident;
- incident outcome (successful compromise, failed attempt, unknown);
- impact to CDI;
- impact on ability to provide operationally critical support;

- DOD programs, platforms or systems involved; and
- any additional information relevant to the incident.

See DOD Industry Day, slide 68 (June 23, 2017); DFARS 252.204-7012(c)(2) (citing *dibnet.dod.mil*). Contractors are to report cyber incidents through the DOD defense industrial base (DIB) website. See DFARS 252.204-7012(c).

> • *Note*: The DFARS provision does not include a requirement for a subcontractor to provide much information regarding cyber incidents to higher-tier subcontractors or the prime contractor. It requires only that the subcontractor provide the next higher-tier contractor with the incident report number assigned by DOD to the subcontractor's incident "as soon as practicable." DFARS 252.204-7012(m)(2)(ii); see DFARS 204.7302(b). This is an area a prime contractor may consider raising with the subcontractor. Prime contractors may consider attempting to obtain subcontractor commitments to report certain cyber incident information within a prescribed period. Many subcontractors will likely be resistant to proposed reporting obligations that exceed those specifically required by regulation. Those who are resistant will nonetheless want to be sure that the reporting triggers are well defined, that the reporting period is adequate, and that their information is protected.

If malicious software is discovered during review of a cyber incident, the contractor must supplement the cyber incident report with information about the malicious software (malware) and provide it to the "DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer." DFARS 252.204-7012(d). The contractor must use the malware submission form (at *https://dcise.cert.org/icf/*), indicate the cyber incident report number, and select the malware to upload and submit. DOD Industry Day, slide 70 (June 23, 2017).

After it receives a cyber incident report, DOD will respond as follows:

(1) DC3 will send the report to the COs identified on the incident collection format (ICF) via encrypted e-mail, and the COs will provide the ICF to the requiring activities;

(2) DC3 will analyze the report to identify cyber threat vectors and adversary trends; and

(3) DC3 will contact the reporting company if the report is incomplete (e.g., no contract numbers, no CO listed).

See DOD Industry Day, slide 67 (June 23, 2017).

Preservation of Media and Damage Assessment—For at least 90 days after reporting a cyber incident, contractors should "preserve and protect images of all known affected information systems" and "all relevant monitoring/packet capture data" discovered during the review. DFARS 252.204-7012(e). The stated purpose of this requirement is "to allow DoD to request the media or decline interest." Id.

DOD may request the preserved media to conduct a "damage assessment" of the incident. DFARS 252.204-7012(g); see DFARS 204.7302(b)(1)(iii). It also may request access to additional information or equipment to conduct a forensic analysis. DFARS 252.204-7012(f); see DFARS 204.7302(b)(1)(iii). The purpose of DOD's damage assessment is to:

- determine the impact of compromised information on U.S. military capability underpinned by the technology;
- consider how the compromised information may enable an adversary to counter, defeat, or reverse engineer U.S. capabilities; and
- focus on the compromised intellectual property impacted by the cyber incident—not on the compromise mechanism.

See DOD Industry Day, slide 72 (June 23, 2017).

The consequences to the contractor after DIB receives notification of a cyber incident and/or following a damage assessment are unclear. In accordance with the "policy" set forth in the DFARS, "A cyber incident that is reported by a contractor or subcontractor shall not, by itself, be interpreted as evidence that the contractor or subcontractor has failed to provide adequate security on their covered contractor information systems, or has otherwise failed to meet the requirements of [DFARS 252.204-7012]." DFARS 204.7302(d). This is seemingly good news for contractors, and seems fair given the well-accepted principle nowadays that "there are only two types of companies—those that have been hacked and those that don't know they have been hacked."

However, the provision adds that COs will consider cyber incidents "in the context of an overall assessment of a contractor's compliance with [DFARS 252.204-7012]." Id. Thus, depending on the severity of

the incident, a cyber incident may lead to a finding of noncompliance or a negative Contractor Performance Assessment Reporting System evaluation, notwithstanding the diligent implementation of reasonable security controls. As explained below, documentation evidencing prompt adherence to a robust response plan following a cyber incident can demonstrate to the CO the reasonableness of the contractor's existing policies and controls for purposes of establishing compliance and providing confidence in continued performance.

Protection and Nondisclosure of Cyber Incident Information—The DFARS states that the Government is to protect from unauthorized disclosure "contractor attributional/proprietary information" provided by a contractor following a cyber incident. DFARS 252.204-7012(h); see DFARS 204.7302(c). "Contractor attributional/proprietary information" is defined as

> information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (*e.g.*, program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

DFARS 252.204-7012(a). Contractors should therefore ensure that information provided to the Government includes clear, appropriate legends. However, the DFARS provision identifies circumstances in which the Government may use and release such data, including release to "entities with missions that may be affected by such information." DFARS 252.204-7012(i)–(j). What happens once the information is released is not clear, although one might assume that the receiving entities should be similarly obligated to protect the information.

DOD may also authorize release of contractor information to support services contractors assisting the Government with forensic analysis, damage assessment or other activities related to safeguarding CDI or reviewing cyber incidents. See DFARS 252.204-7012(i)(5). These contractors are subject to strict nondisclosure requirements for information "obtained from a third party's reporting of a cyber incident" pursuant to DFARS 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

A support services contractor must protect the information and use it only to assist the Government under a contract related to safeguarding CDI or cyber incident reporting. DFARS 252.204-7009(b)(1)–(2). Further, it must execute employee nondisclosure agreements to which the contractor that provided the information is a third-party beneficiary. DFARS 252.204-7009(b)(3)–(4). The DFARS provision provides severe penalties, including criminal and civil actions by the U.S., as well as "appropriate remedies" for the contractor that provided the information, if support services contractors violate the use and nondisclosure provision. DFARS 252.204-7009(b)(5). The clause is to be flowed down to subcontractors providing similar Government support services. DFARS 252.204-7009(c).

Cyber Incident Response Plan—The contractor's system security plan should include procedures for monitoring and responding to a data breach or cyber incident. When a potential cyber incident is detected, the contractor should attempt first to identify and isolate the affected systems and devices in order to minimize further damage. The plan should include a process to identify the responsible individuals and steps to be taken to determine what constitutes a "cyber incident" for DOD reporting purposes. Malware should be identified and, if appropriate, sent to DOD as noted above.

After the immediate threat is contained and reported, the contractor should examine the cyber incident and use it to inform future security practices. It should identify other systems or devices with similar vulnerabilities, and modify its security plan and controls to facilitate enhanced protections. Obviously, the source of the problem must be investigated. If the cyber incident results from an employee's unintentional action, more rigorous training and potential employee sanctions should be considered. The contractor also should document steps taken to review and correct a problem following a cyber incident. This documentation may come into play later to support the reasonableness of the contractor's actions and to provide proof of contractor fitness to continue to perform under contracts requiring security control compliance.

- *Note*: NIST SP 800-171 includes the following security requirements relating to identification,

Table 1: NIST SP 800-171 Security Requirements Relating to Identification, Documentation, and Reporting of Cyber Incidents

3.3	**Audit and Accountability**
3.3.1	Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.
3.6	**Incident Response**
3.6.2	Track, document, and report incidents to appropriate officials and/or authorities both internal and external to the organization.
3.14	**System and Information Integrity**
3.14.1	Identify, report, and correct information and system flaws in a timely manner.

documentation and reporting of cyber incidents. See Table 1 above.

Conclusion—If past is prologue (and it often is), there is little doubt that even with appropriate security controls in place, a contractor will experience at some point a cyber attack or other cyber incident. A sound and comprehensive response plan created with a thorough understanding of the reporting requirements will allow a contractor to minimize the informational damage associated with a cyber incident, and limit other negative consequences. The reasonableness of the contractor's actions once a cyber incident is detected, demonstrated through detailed documentation that can be provided to the Government, will no doubt be examined to determine the capabilities of the contractor, its past performance, and its continuing eligibility to receive future work.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* John Chierichella *and* Townsend Bourne. *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 International Trade practice group, and co-leader of the firm's Aerospace and Defense Industry team. Ms. Bourne is an associate in Sheppard Mullin's Washington, D.C. office and a member of the Government Contracts, Investigations, and International Trade practice group. They can be reached at jchierichella@sheppardmullin.com and tbourne@sheppardmullin.com, respectively.