THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 60, No. 26 **July 18, 2018**

Focus

¶ 215

FEATURE COMMENT: Federal Information Systems Reside In A Glass House ... And Several Other Reasons Why The Government Should Exercise Caution, Cooperation And Flexibility When Enforcing Cybersecurity Regulations—Part I

Introduction—The Office of Management and Budget recently published a "Federal Cybersecurity Risk Determination Report and Action Plan" reflecting a Government-wide cybersecurity risk assessment conducted by OMB in coordination with the Department of Homeland Security. OMB, *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018) (OMB report), available at *www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf*.

The results were not good. OMB and DHS determined that a majority of agencies assessed "have cybersecurity programs that are either at risk or high risk." Id. at 3. Among other findings, the report flatly notes that "[a]gencies do not understand and do not have the resources to combat the current threat environment." Id. at 6. The OMB report is only one of several Government publications highlighting the dire state of agency cyber defenses. What these publications underscore is that compliance with cybersecurity requirements is neither easy nor instantaneous, and that, with respect to cybersecurity, Government information systems reside in a "glass house."

Government contractors and subcontractors understand both the difficulties posed by the requirements and the current predicament of achieving compliance. In 2016, the Government imposed many costly and burdensome cybersecurity requirements on contractors and subcontractors, who are working hard to develop the policies, procedures and systems to comply with the cybersecurity regulations.

As discussed below, the Government's failure to protect its information systems is one of several compelling reasons why the Government should proceed with caution, cooperation and flexibility in overseeing the implementation and enforcement of the contractor cybersecurity regulations. Asking the Government to consider all of these reasons when deciding when and how to exercise its formidable powers is not asking the Government to abandon its right to compliance with contract terms.

Rather, it is asking the Government to recognize the unique difficulties, complexities and ambiguities in cybersecurity regulations that are focused on a 21st century problem affecting organizations around the globe—including federal agencies. The Government, of course, has an implied duty of good faith and fair dealing, and the duty to cooperate is part of that implied duty. *Agility Pub. Warehousing Co. KSCP v. Mattis*, 852 F.3d 1370, 1383–84 (Fed. Cir. 2017); 59 GC ¶ 112. Cooperation between the Government and its contractors will be critical to successful implementation of these regulations.

This Feature Comment is presented in two parts. Part I summarizes the 2016 cybersecurity regulations, and discusses the OMB report and other Government publications acknowledging material problems that afflict federal cybersecurity capabilities. Part II gives several reasons why the Government should proceed with caution, cooperation and flexibility when enforcing cybersecurity regulations.

The 2016 Cybersecurity Regulations—2016 was a watershed year for contractor cybersecurity regulations because the Government enacted three significant sets of regulations: amendments to the Federal Acquisition Regulation and the Defense FAR Supplement, as well as regulations covering controlled unclassified information (CUI). These regulations are discussed below.

The FAR Amendments: In May 2016, the Department of Defense, General Services Administration and NASA amended the FAR to add a new subpart and contract clause covering the "basic safeguarding of contractor information systems that process, store or transmit Federal contract information." 81 Fed. Reg. 30439 (May 16, 2016). The amendments added a new subpt. 4.19, "Basic Safeguarding of Covered Contractor Information Systems," and a new clause at FAR 52.204-21. Subpt. 4.19 applies to all acquisitions, including acquisitions of commercial items other than commercially available off-the-shelf (COTS) items, if a contractor's information system "may" contain "Federal contract information." FAR 4.1902. FAR 4.1901 defines "Federal contract information" as "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 it excludes information provided by the Government to the public or "simple transactional information, such as that necessary to process payments." The new clause at FAR 52.204-21 imposes numerous safeguarding requirements on contractors and subcontractors.

The CUI Regulations: In September 2016, the National Archives and Records Administration promulgated 32 CFR pt. 2002, covering CUI. These regulations apply "indirectly" to nonexecutive branch CUI recipients through agreements (32 CFR § 2002.1(f)), and specify that such agreements must state that (1) the recipient handle CUI in accordance with Executive Order (EO) 13556, pt. 2002, and the CUI Registry (an online CUI repository), and (2) misuse of CUI is subject to penalties established in applicable laws, regulations and Government-wide policies (32 CFR § 2002.16(a)(6)).

Part 2002 specifies that National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting [CUI] in Nonfederal Systems and Organizations," defines the requirements necessary to protect "CUI Basic" on non-Federal information systems. See 32 CFR § 2002.14(h)(2). CUI Basic is one of two main categories of CUI established in pt. 2002, and is "the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in this part and the CUI Registry." 32 CFR § 2002.4(j).

The CUI Registry is an online repository for all information, guidance, policy and requirements on handling CUI. 32 CFR § 2002.4(p). The other main category of CUI is "CUI Specified," for "which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic." The CUI Registry specifies which laws, regulations and Government-wide policies include such specific requirements. 32 CFR § 2002.4(r).

The DFARS Amendments: In October 2016, DOD enacted a final rule amending the DFARS to specify that "adequate security" is required on all "covered contractor information systems." 81 Fed. Reg. 72986, 72988 (Oct. 21, 2016). (The Oct. 21, 2016 DFARS amendments were the culmination of a process that began with a final rule in 2013 (78 Fed. Reg. 69273 (Nov. 18, 2013)), two interim rules (80 Fed. Reg. 51739 (Aug. 26, 2015) and 80 Fed. Reg. 81472 (Dec. 30, 2015)) and comments on the interim rules.) The clause at DFARS 252.204-7012, which must be included in all solicitations and contracts except those solely for COTS items (DFARS 204.7304(c)), defines "covered contractor information system" as "an unclassified information system that is owned, or operated by or for, a contractor that processes, stores, or transmits covered defense information." DFARS 252.204-7012(a). "Covered defense information" (CDI) means:

> unclassified controlled technical information or other information, as described in the [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 Governmentwide 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 252.204-7012(a). For "covered contractor information systems" that are not part of an information technology service or system operated on behalf of the Government, adequate security means that the covered contractor information system is subject to the security requirements in NIST SP 800-171 in effect when the solicitation is issued or as authorized by the contracting officer. DFARS 252.204-7012(b)(2).

These regulations impose a multitude of requirements on contractors. The CUI and DFARS cybersecurity provisions are particularly onerous—NIST SP

800-171 contains *110 security requirements*. NIST SP 800-171, Rev. 1, at 9–15 (December 2016) (includes updates as of June 7, 2018), available at *nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf*. Also, pursuant to DFARS 252.204-7012, if a contractor discovers a "cyber incident" that affects a covered contractor information system or the CDI residing therein, the contractor must report a large amount of information concerning the cyber incident to DOD within 72 hours of the discovery. See DFARS 252.204-7012(c)(ii). The commentary accompanying the 2016 final DFARS rule acknowledges that "[f]or a new contractor that has not been subject to the previous iteration of the 252.204-7012 clause and is now handling [CDI,] *the cost could be significant to comply*." 81 Fed. Reg. 72986, 72997 (October 2016) (emphasis added).

Also, the regulations discussed above are in addition to cybersecurity regulations that have been enacted and proposed by other agencies, such as the clause at 48 CFR § 3052.204-70 that must be included in DHS contracts requiring submission of an IT security plan.

OMB's Federal Cybersecurity Risk Determination Report and Action Plan—*Overview*: The May 2018 OMB report is one of the most recent formal acknowledgements by the Government that the status of cybersecurity *within the Government itself* leaves much to be desired. OMB prepared the report in response to EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, which President Trump issued on May 11, 2017. That order required each agency to provide a "risk management report" to the DHS secretary and OMB director within 90 days. The order acknowledged problems with the Government's cybersecurity, noting that "[t]he executive branch has for too long accepted antiquated and difficult-to-defend IT," and "[k]nown but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies.... Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance." EO 13800 (May 11, 2017).

Pursuant to the EO, OMB and DHS conducted a Government-wide cybersecurity risk assessment, examining the performance of 96 agencies across 76 "metrics." OMB report at 3. The results reflect material, systemic problems that should be of concern to every U.S. citizen. The report states that "OMB and DHS determined that 71 of 96 agencies (74 percent) participating in the risk assessment process have cybersecurity programs that are either at risk or high risk."

In addition, OMB and DHS found that agencies are not equipped to determine how threat actors seek to gain access to their information, that the lack of threat information results in ineffective allocations of agencies' limited cyber resources, and that this situation "creates enterprise-wide gaps in network visibility, IT tool and capability standardization, and common operating procedures, all of which negatively impact Federal cybersecurity." Id.

Finding 1: The OMB report includes four broad "findings" about agency cybersecurity problems, and includes detailed descriptions of the findings. The first finding is damning: "Agencies do not understand and do not have the resources to combat the current threat environment." Id. at 6. The report notes that agencies are not keeping pace with escalating cyber attacks—while threat actors employ persistent and increasingly sophisticated attack techniques, agencies' ability to determine the actors' motivations and attack methods has not improved. The report further notes that "situational awareness is so limited that Federal agencies could not identify the method of attack, or attack vector, in 11,802 of the 30,899 cyber incidents (38 percent) that led to the compromise of information or system functionality in [fiscal year] 2016." Id.

These facts are troubling, and it is worth emphasizing that agencies experienced *over 30,000 compromising cyber incidents in one year alone*. Moreover, the fact that agencies "often lack timely information regarding the tactics, techniques, and procedures that threat actors use to exploit government information systems" stands in sharp contrast to the requirement in DFARS 252.204-7012 to "rapidly report"—i.e., within 72 hours of discovering a cyber incident—a description of the technique or method used in the incident. See DFARS 252.204-7012(c)(2) (requiring contractors to report elements at *dibnet.dod.mil/portal/intranet/*; those elements are set forth at that website at "For DoD Contractors" under "Reporting a Cyber Incident").

Finding 2: "Agencies do not have standardized cybersecurity processes and IT capabilities, which impacts their ability to efficiently gain visibility and effectively combat threats." OMB report at 12. The report explains that "[*f*]*undamentally, any organization must have a clear understanding of the people, assets, and data on*

its networks," and agencies employ fragmented identity, credential and access management programs, which "*prevent*[] *agencies from achieving a comprehensive understanding of their users, managing those users' access to the agency network, and effectively safeguarding sensitive government information*." Id. at 12–13 (emphasis added).

Although the Government struggles to understand its users and manage user access to agency networks, the 2016 FAR rule imposed similar requirements on contractors. For example, that rule requires contractors to "[i]dentify information system users, processes acting on behalf of users, or devices." FAR 52.204-21(b)(v). That rule also requires contractors to "[l]imit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)" (FAR 52.204-21(b)(i)), and to "[l] imit information system access to the types of transactions and functions that authorized users are permitted to execute" (FAR 52.204-21(b)(ii)). All three of these security requirements are specified in NIST SP 800-171 (Rev. 1, at 9, 11), which (as discussed above) applies to contractors in certain circumstances pursuant to DFARS 252.204-7012 and the 2016 CUI rule.

Finding 3: "Agencies lack visibility into what is occurring on their networks, and especially lack the ability to detect data exfiltration." OMB report at 15. The report explains that "agencies do not have the visibility into their networks to effectively detect data exfiltration attempts *and respond to cybersecurity incidents. The risk assessment revealed that 73 percent of agency programs are either at risk or high risk in this critical area*." Id. (emphasis added). Moreover, agency inspectors general found that "only 30 percent of agencies have predictable, enterprise-wide incident response processes in place, *with as few as 17 percent of agencies actually analyzing incident response data after an incident has occurred*." Id. (emphasis added). The report characterizes this situation as "untenable" because "agencies *lack both the visibility into their networks to determine the occurrence of cybersecurity incidents and the ability to minimize the impact of an incident if one is detected*." Id. (emphasis added).

These substantial problems associated with such an important aspect of cybersecurity—responding to cyber incidents—are deeply troubling. And they create a significant disparity between the Government's cyber reporting failures and the Government's demands that contractors report cyber incidents, particularly the reporting requirements in DFARS 252.204-7012. Under this provision, contractors must report a large amount of information within 72 hours of discovering a cyber incident, including, but not limited to, the impact to CDI; the location(s) of compromise; the DOD programs, platforms or systems involved; the type of compromise, i.e., unauthorized access, unauthorized release (includes inadvertent release), unknown or not applicable; a description of the technique or method used in the incident; the incident outcome, i.e., successful compromise, failed attempt or unknown; and an "incident/compromise narrative." See DFARS 252.204-7012(c)(2) (requiring contractors to report elements at *dibnet.dod.mil/portal/intranet/*; the elements are set forth at that website at "For DoD Contractors" under "Reporting a Cyber Incident"). Additionally, NIST SP 800-171—applicable to contractors in certain circumstances pursuant to DFARS 252.204-7012 and the 2016 CUI rule—sets forth incident response security requirements, including establishment of an operational incident-handling capability that includes adequate preparation, detection, analysis, containment, recovery and user response activities. NIST SP 800-171, Rev. 1, at 12.

Finding 4: "Agencies lack standardized and enterprise-wide processes for managing cybersecurity risks." OMB report at 17. This is ironic, given that the 2016 regulations impose substantial standardized processes on contractors for managing cybersecurity risks. The commentary accompanying the fourth finding indicates that "awareness and accountability for managing cybersecurity risks [are] uneven across the Federal enterprise," and "Federal agencies possess neither robust risk management programs nor consistent methods for notifying leadership of cybersecurity risks across the agency." Id.

The foregoing facts establish that substantial problems exist in federal agency cybersecurity. And the OMB report indicates that there are other problems in addition to the four findings. Specifically, the report does not cover every risk identified in the risk assessments submitted by agencies, and "[t]wo of the most significant areas of risk that were identified in agency assessments were the abundance of legacy [IT], which is difficult and expensive to protect, as well as shortages of experienced and capable cybersecurity personnel." OMB report at 2. The importance of the OMB report cannot be overstated—it was mandated by executive order, and reflects significant input from individual agencies, as analyzed by OMB and DHS during the one-year period following the EO.

Further Evidence of Problems—Yet the OMB report is only one of the latest acknowledgements that material problems plague the Government's cybersecurity capabilities. For example, in February 2017, the Government Accountability Office issued a report on cybersecurity actions needed to strengthen U.S. capabilities. The first sentence of that report states, "GAO has consistently identified shortcomings in the federal government's approach to ensuring the security of federal information systems and cyber critical infrastructure as well as its approach to protecting the privacy of personally identifiable information (PII)." *Cybersecurity—Actions Needed to Strengthen U.S. Capabilities*, at highlights page, available at *www.gao.gov/assets/690/682756.pdf*. The report further states that systems used by agencies "are often riddled with security vulnerabilities—both known and unknown. For example, the national vulnerability database maintained by [NIST] has identified 82,384 publicly known cybersecurity vulnerabilities and exposures as of February 9, 2017, with more being added each day." Id. at 2–3.

In addition, GAO noted that in the last several years, it had made approximately 2,500 recommendations to agencies to improve the security of federal systems and information. However, GAO explained that "many agencies continue to be challenged in safeguarding their information systems and information, in part because many of these recommendations have not been implemented. As of February 2017, about 1,000 of our information security-related recommendations had not been implemented." Id. at 5. GAO also noted that "[i]n April 2014 we reported that 24 major federal agencies did not consistently demonstrate that they had effectively responded to cyber incidents." Id. at 9.

In September 2017, GAO issued another report finding that in FY 2016, federal agencies continued to experience weaknesses in protecting the information systems due to ineffective implementation of security policies and practices. *Federal Information Security—Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices*, at highlights page, available at *www.gao.gov/assets/690/687461.pdf.* The report noted that agency IGs evaluated agency information security programs and determined that most agencies did not have effective information security program functions in FY 2016. Id. at 37. And GAO did not bother making any new recommendations because GAO and the IGs had previously made hundreds of recommendations. Id. at 46.

In May of this year, DHS issued its "Cybersecurity Strategy" pursuant to § 1912 of the 2017 National Defense Authorization Act. DHS, Cybersecurity Strategy (May 15, 2018), available at *www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf*. One of seven goals in that strategy is to "reduce vulnerabilities of federal agencies to ensure they achieve an adequate level of cybersecurity" (id. at 8), which is an acknowledgement that the cybersecurity of federal agencies is inadequate.

The strategy explains that "[a]ttempted incursions into government networks occur on a daily basis; the number of cyber incidents on federal systems reported to DHS increased more than ten-fold between 2006 and 2015." Id. at 2. In issuing the strategy, the DHS secretary stated that "the cyber threat landscape is shifting in real-time, and we have reached a historic turning point.... [I]t is clear that our cyber adversaries can now threaten the very fabric of our republic itself." Press release, Department of Homeland Security Unveils Strategy to Guide Cybersecurity Efforts (May 15, 2018), available at *www.dhs.gov/news/2018/05/15/department-homeland-security-unveils-strategy-guide-cybersecurity-efforts*.

With all of these problems, contractors would be justified in worrying that the Government may not be able to protect confidential and proprietary business data that contractors submit to agencies. Contractors also may note the irony of the Government imposing multiple cybersecurity procurement regulations.

This concludes Part I of this Feature Comment. Part II will appear in next week's edition of THE GOVERNMENT CONTRACTOR, and will discuss the many reasons why the Government should exercise caution, cooperation and flexibility when enforcing cybersecurity procurement regulations.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Cameron S. Hamrick, *a Principal at Miles & Stockbridge P.C. in the firm's Washington, D.C. office. ***Disclaimer: This is for general information and is not intended to be and should not be taken as legal advice for any particular matter. It is not intended to and does not create any attorney-client relationship. The opinions expressed and any legal positions asserted in the article are those of the author and do not necessarily reflect the opinions or positions of Miles & Stockbridge P.C. or its other lawyers.***