THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 60, No. 27 **July 25, 2018**

Focus

¶ 221

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 II

This is the second part of a two-part article discussing several reasons why the Government should exercise caution, cooperation and flexibility when enforcing cybersecurity procurement regulations, including reasons arising from the fact that the Government has imposed numerous burdensome cybersecurity regulations on contractors and subcontractors despite formally acknowledging the alarming state of the Government's efforts to protect agency information systems—meaning that Government information systems reside in a "glass house."

Part I, which ran in THE GOVERNMENT CONTRACTOR last week, summarized the following cybersecurity procurement regulations promulgated in 2016: regulations covering controlled unclassified information (CUI) and amendments to the Federal Acquisition Regulation and Defense FAR Supplement. Part I also discussed a report published by the Office of Management and Budget, *Federal Cybersecurity Risk Determination Report and Action Plan* (OMB report, available at *www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf*), as well as other Government publications, acknowledging material deficiencies in agency cyber defenses. See 60 GC ¶ 215. Part II discusses several reasons why the Government should exercise caution, cooperation and flexibility when enforcing cybersecurity procurement regulations.

The Many Reasons Why Caution, Cooperation and Flexibility Are Prudent—The 2016 regulations do not specify particular administrative remedies or penalties for noncompliance (as noted in Part I, the CUI regulations state that misuse of CUI is subject to penalties established in applicable laws, regulations or Government-wide policies). As the Department of Defense has acknowledged, the DFARS cybersecurity regulations "did not change the existing penalties or remedies for noncompliance with contract requirements." See DOD, "Frequently Asked Questions regarding DFARS Subpart 204.73 and PGI Subpart 204.73[,] DFARS Subpart 239.76 and PGI Subpart 239.76," at 19 (April 2, 2018), available at *dodprocurementtoolbox.com/cms/sites/default/files/resources/2018-04/Revision%20to%20Cyber%20DFARS%20FAQs%20-%20April%202%202018.pdf*.

The Government possesses a formidable array of remedies, sanctions and penalties when it conducts business with private entities—including but not limited to negative past performance assessments, terminations for default, suspension and debarment, and civil and criminal false claims. However, there are multiple compelling reasons—discussed below—why the Government should exercise caution before resorting to the more powerful weapons at its disposal as it oversees implementation of cybersecurity regulations. Indeed, the Government would be well-advised to proceed with cooperation and flexibility when addressing contractor compliance with, and Government enforcement of, cybersecurity procurement requirements.

The Government's Cybersecurity Difficulties Are Part of a Larger Problem That Affects Federal Contractors and Subcontractors: The fact that the Government's attempts to protect its own information systems against unauthorized intrusions are riddled with multiple difficulties and gaps is a reflection of a larger problem—dealing with these types of attacks is a substantial dilemma

for everyone. Simply mandating that contractors and subcontractors comply with many cybersecurity requirements will not eliminate this dilemma in Government procurements.

Compliance with Cybersecurity Regulations Requires Technical Expertise: Moreover, the cybersecurity regulations require specialized technical skills to implement and perform, and such skills are not readily available. As OMB explained in 2016, the supply of cybersecurity talent to meet the Government's increasing demand is not sufficient, and this shortfall affects not only the Government, but the private sector as well. OMB, *Strengthening the Federal Cybersecurity Workforce* (July 12, 2016), available at *obamawhitehouse.archives.gov/blog/2016/07/12/strengthening-federal-cybersecurity-workforce*. See also White House, "Delivering Government Solutions In the 21st Century[,] Reform Plan and Reorganization Recommendations" at 108 (June 21, 2018), available at *www.whitehouse.gov/wp-content/uploads/2018/06/Government-Reform-and-Reorg-Plan.pdf* ("The Federal Government struggles to recruit and retain cybersecurity professionals due to a shortage of, and growing demand for, cybersecurity talent across the public and private sectors.").

A recent report by the secretaries of commerce and homeland security states that there were an estimated 299,000 openings for cybersecurity-related jobs in the U.S. as of August 2017, with global projections suggesting a cybersecurity workforce shortage of 1.8 million by 2022. The report bluntly notes that "[c]ompetition for qualified cybersecurity workers is intense across all sectors." *A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future* at 1 (May 10, 2018), available at *www.nist.gov/sites/default/files/documents/2018/05/10/eo_wf_report_to_potus.pdf*.

Nor does the pervasive demand for cybersecurity specialists come cheap even if contractors are fortunate enough to find the requisite talent—pay for cybersecurity jobs tends to be above the average levels for other positions in many parts of the economy. Id. Because contractors and subcontractors may experience difficulties finding and retaining skilled professionals necessary to comply with cybersecurity regulations, the Government should work with its contractors to address issues that arise from the regulations, as opposed to blindly and harshly enforcing compliance.

The Government Is Not Complying with its Cybersecurity Obligations: Further, unreasonably harsh or knee-jerk enforcement of these regulations would be difficult to square with the fact that the Government is not complying with its own cybersecurity obligations. The Government must comply with the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA). (The Federal Information Security Management Act of 2002 is at Title III of the E-Government Act of 2002, P.L. 107-347, 116 Stat. 2899 (2002); the Federal Information Security Modernization Act of 2014 is P.L. 113-283, § 2, 128 Stat. 3073 (2014) (codified at 44 USCA §§ 3551–3558)). FISMA imposes several requirements on agencies, including that agencies provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification or destruction of information systems used or operated by the agency. 44 USCA § 3554(a)(1)(A). A September 2017 Government Accountability Office report (discussed in Part I) noted that agencies must comply with FISMA. *Federal Information Security Weaknesses Continue to Indicate Need for Effective Implementation of Policies and Practices* (GAO-17-549) at highlights page (September 2017) (GAO September 2017 report), available at *www.gao.gov/assets/690/687461.pdf*; see also id. at 12–13. Similarly, GAO noted that it prepared the report pursuant to the FISMA provision requiring GAO to report periodically to Congress on agencies' implementation of the Act. See id. at 3. Yet that report indicated that agencies are not complying with their obligations: "While federal agencies are working to carry out their FISMA-assigned responsibilities, they continue to experience information security program deficiencies and security control weaknesses in all areas." Id. at 46. The report also noted that weaknesses in security controls indicate that agencies did not adequately or effectively implement information security policies and practices during fiscal year 2016. Id. at 15; see also id. ("Further, our work and reviews by inspectors general highlighted information security control deficiencies at agencies that expose information and information systems supporting federal operations and assets to elevated risk of unauthorized use, disclosure, modification, and disruption.").

Enforcement of the Government's Cybersecurity Compliance is Tepid: Harsh or aggressive enforce-

ment of contractor cybersecurity regulations also would be difficult to reconcile with the lax enforcement of Government cybersecurity compliance. Notwithstanding repeated identification of weaknesses, agencies are not held accountable for failing to comply with FISMA. Smith, "Hacking Federal CyberSecurity Legislation: Reforming Legislation to Promote the Effective Security of Federal Information Systems," 4 Nat'l Sec. L.J. 345, 374 (2016). As Rep. Lamar Smith (R-Texas) stated, "Too many federal agencies like [the Office of Personnel Management] fail to meet the basic standards of cybersecurity, and no one is being held accountable." Id. (citing Zach Noble, "Fixing FISMA, Blaming ... Someone, and Another Lawsuit," FCW: The Bus. Of Fed. Tech. (July 9, 2015), available at *fcw.com/articles/2015/07/09/opm-breach-hearing.aspx* (quoting Rep. Smith)).

Also it is difficult to conclude that agencies are being aggressively "policed" on adequate cybersecurity, given information, discussed in Part I of this series, from a February 2017 GAO report indicating that roughly 1,000 GAO recommendations to agencies had not been implemented. *Cybersecurity Actions Needed to Strengthen U.S. Capabilities* (GAO-17-440T) at highlights page (Feb. 14, 2017), available at *www.gao.gov/assets/690/682756.pdf*, see also GAO September 2017 report at 46 ("We are not making new recommendations to address these weaknesses because we and the inspectors general have previously made hundreds of recommendations."). As GAO explained in the September 2017 report, "Until agencies correct *longstanding deficiencies and address our and agency inspectors general's recommendations*, federal IT systems will remain at increased and unnecessary risk of attack or compromise." GAO September 2017 report at 46 (emphasis added).

Complying with the Cybersecurity Regulations Can Be Difficult, and the DFARS and CUI Regulations Are Unquestionably Burdensome: Complying with the cybersecurity regulations discussed in this Feature Comment is not easy. The FAR requirements can present difficulties for contractors and subcontractors because the clause at 52.204-21 imposes numerous safeguarding requirements. The difficulties involved in implementing and complying with these requirements can be seen in the fact that the Government has trouble complying with some of these requirements. For example, one of the FAR requirements is "Update malicious code protection mechanism when new releases are available." FAR 52.204-21(b)(1)(xiv). Yet the May 2017 executive order discussed in Part I noted that known agency vulnerabilities include declining to implement a vendor's security patch. EO 13800 (May 11, 2017). Similarly, another FAR requirement is "Identify information system users, processes acting on behalf of users, or devices." FAR 52.204-21(b)(1)(v). However, the OMB report explains that, across Government, agencies employ a structure that prevented them from achieving a comprehensive understanding of their users and managing those users' access to the agency network. OMB, *Federal Cybersecurity Risk Determination Report and Action Plan* at 13 (May 2018), available at *www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf*.

Turning to the CUI and DFARS cybersecurity rules, those rules require compliance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting [CUI] in Nonfederal Systems and Organizations," a publication that was discussed in Part I. NIST SP 800-171, Rev. 1, available at *nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf*. The CUI regulations require compliance with NIST SP 800-171 to protect "CUI Basic," one of two main categories of CUI established in 32 CFR pt. 2002 (discussed in Part I), on non-federal information systems. See 32 CFR § 2002.14(h)(2). The DFARS cybersecurity rules require compliance with NIST SP 800-171 for covered contractor information systems that are not part of an IT service or system operated on behalf of the Government. See DFARS 252.204-7012((b)(2)(i). Compliance with NIST SP 800-171 is burdensome. That publication has over 100 pages and specifies 110 different security controls, grouped into 14 security requirement "families." As explained previously, the Government is struggling to comply with requirements like those specified in NIST SP 800-171. For example, agency IGs have determined 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." OMB report at 15. These Government struggles are evidence of the difficulties posed by the NIST controls. However, the Government expects certain contractors and subcontractors to comply with NIST SP 800-171, which sets forth incident response security requirements. NIST SP 800-171, Rev. 1, at 12.

Furthermore, in February of this year, NIST released a final draft of SP 800-171A, "Assessing Security Requirements for [CUI]," for public comment. Draft NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" (February 2018), available at *csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/sp800-171A-draft.pdf*. That publication provides assessment procedures and a methodology that can be used to conduct assessments of the security requirements in NIST SP 800-171. Id. at ii. Organizations can use the assessment procedures to generate evidence that the security requirements have been satisfied. Id. at 2. The draft publication is commendable; however, the fact that the draft is over *120 pages long*—longer than SP 800-171—is striking, and demonstrates the complexities and burdens associated with complying with SP 800-171.

Similarly, DOD has issued publications attempting to address the requirements of the DFARS cybersecurity rules, but these publications also reflect the onerous nature of the requirements. In January 2017, DOD issued 59 "Frequently Asked Questions" regarding DFARS cybersecurity provisions. "Frequently Asked Questions regarding DFARS Subpart 204.73 and PGI Subpart 204.73[,] DFARS Subpart 239.76 and PGI Subpart 239.76" (Jan. 27, 2017), available at *www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf*. Yet that large number of questions and answers was insufficient, and in April of this year, DOD revised the document by issuing a *58-page, single-spaced set of 109* "Frequently Asked Questions." "Frequently Asked Questions regarding DFARS Subpart 204.73 and PGI Subpart 204.73[,] DFARS Subpart 239.76 and PGI Subpart 239.76" (April 2, 2018) (FAQs). The FAQs are helpful, but the multitude of questions and answers only underscores the complexities, ambiguities and burdensome nature of the DOD rules. Here is one example from the FAQs:

> **Q68 (Q35/Q36): Security Requirements 3.1.13, 3.1.17, 3.1.19, 3.13.8, and 3.13.11—Do all of the 171 security requirements for cryptography have to be [Federal Information Processing Standard (FIPS)] validated, and if so, what does that mean? If the algorithm is FIPS approved, is that sufficient?**
>
> A68 Yes, all the NIST SP 800-171 requirements for cryptography used to protect the confidentiality of CUI (or in this case covered defense information [CDI]) must use FIPS-validated cryptography, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient—the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. When an application or device allows a choice (by selecting FIPS-mode or not), then the FIPS-mode has been validated under FIPS 140-2, but the other options (non-FIPS) allow certain operations that would not meet the FIPS requirements. More information is available at http://crsc.nist.gov/groups/STM/CMVP/ and http://crsc.nist.gov/groups/STM/cmvp/validation.html.
>
> When NIST SP 800-171 requires cryptography, it is to protect the confidentiality of CUI (or in this case covered defense information). Accordingly, FIPS-validated cryptography is required to protect CUI, typically when transmitted or stored outside the protected environment of the covered contractor information system (including wireless/remote access) if not separately protected (e.g., by a protected distribution system). FIPS validated cryptography is required whenever the encryption is required to protect covered defense information in accordance with NIST SP 800-171 or by another contract provision. Encryption used for other purposes, such as within application or devices within the protected environment of the covered contractor information system, would not need to be FIPS-validated. Note that any separate contract requirement (not currently in NIST SP 800-171) to encrypt data at rest (e.g., PII) within the information system would require use of FIPS validated cryptography.

FAQs at 42–43. Not all contractors and subcontractors will have someone readily available who can understand and implement each element of this single FAQ.

DOD has engaged in other laudable efforts to publicize guidance concerning the DFARS cybersecurity requirements, but these efforts also emphasize the hardships imposed on contractors and subcontractors. For instance, DOD held an industry information day on June 23, 2017, to discuss the DFARS cybersecurity regulations. See, e.g., 82 Fed. Reg. 16577 (April 5, 2017) (providing notice of meeting). The director, Defense Pricing/Defense Procurement and Acquisi-

tion Policy issued a memorandum providing guidance for acquisition personnel concerning DFARS 252.204-7012, dated Sept. 21, 2017. Memorandum from Shay Assad, Dir., DPAP, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" (Sept. 21, 2017) (Assad memo), available at *dodprocurementtoolbox.com/cms/sites/default/files/resources/2017-09/USA002829-17-DPAP.pdf*. And in April 2018, DOD issued draft guidance for procurements requiring implementation of NIST SP 800-171 for public comment. 83 Fed. Reg. 17807 (April 24, 2018). Again, the fact that DOD is devoting a considerable amount of time and attention to the DFARS cybersecurity rules is strong evidence that the rules impose significant burdens on contractors and subcontractors.

Further, the cybersecurity requirements are particularly painful for small businesses. The commentary accompanying the 2016 DFARS rule notes that "[m]ultiple respondents requested that, due to the high cost of compliance, DoD provide for an alternative approach for small business." 81 Fed. Reg. 72986, 72987 (Oct. 21, 2016). DOD did not provide for an alternative approach for small business. And the Small Business Administration's Office of Advocacy commented that the cost of complying with the new rule will be a "significant barrier" to small businesses engaging in federal acquisitions, and many small businesses will be forced to buy services and software to provide adequate safeguards for CDI and to assess their security controls and information systems. 81 Fed. Reg. 72986, 72997 (Oct. 21, 2016).

Because of these burdens, DOD should work with individual contractors to address the difficulties and ambiguities posed by the DFARS rules. See, e.g., draft "DoD Guidance for Reviewing System Security Plans and the NIST 800-171 Security Requirements Not Yet Implemented" at 1 (stating that the guidance "provides clarifying information for security requirements that are frequently misunderstood.") (instructions for accessing document are at 83 Fed. Reg. 17807, 17808 (April 24, 2018)).

For example, contractors and subcontractors are having trouble with the definition of covered defense information, or CDI, at DFARS 252.204-7012(a) (discussed in Part I). Although one part of the definition reasonably requires the Government to mark information as CDI, another part of the definition covers certain information that is "[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract." This second part of the definition raises several questions. The FAQs (Question 19) state that the contracting officer must ensure that "the contract, task order, or delivery order includes the requirement, as provided by the requiring activity (such as a contract data requirements list) for the contractor to mark [CDI] developed in the performance of the contract," while adding the disquieting statement that "[t]he prime is responsible for safeguarding of [CDI] throughout its entire supply chain." FAQs at 19.

Yet telling contractors that they must mark CDI is less than helpful in determining what constitutes CDI. The FAQs (Question 22) also state that marking requirements will "typically" be in Block 9 of the Contract Data Requirements List (CDRL), and that if the contract does not contain a CDRL, the marking requirements "may" be found in Section C. FAQs at 20. This is not sufficient—DOD needs to step up and establish what constitutes CDI in all contracts in a manner that will avoid unnecessary disputes.

DOD also should exhibit reasonable flexibility in overseeing implementation of the DFARS rules. For example, the DFARS provides mechanisms for contractors to request alternatives to NIST SP 800-171 security controls and determinations that a control is not applicable, both prior to award (DFARS 252.204-7008(c)(2)) and after award (DFARS 252.204-7012(b)(2)(ii)(B)). These provisions state that an authorized representative of the DOD chief information officer will "adjudicate" such contractor requests. This smacks of an adversarial relationship. Instead of rejecting contractor requests by written "adjudication," DOD should first engage in a meaningful dialogue with the contractor to explore the proposal and work together in a way that permits the contractor to refine its proposal to address any DOD concerns. The commentary accompanying the Oct. 21, 2016 DFARS amendments indicates, for pre-award variance requests, that if "the DoD CIO needs additional information, a request is made to the contracting officer." 81 Fed. Reg. 72986, 72990 (Oct. 21, 2016). This is helpful, but unnecessarily formal—technical personnel from both parties should discuss the request directly in order to permit the contractor to explain and revise (if necessary) its position.

The Cybersecurity Regulations Are Relatively New: Cybersecurity requirements constitute a relatively new area of federal procurement law. The burdensome requirement in the DFARS to comply with NIST SP

800-171 is a particularly recent requirement—contractors had until the end of last year to implement NIST SP 800-171. See DFARS 252.204-7012(b)(2)(ii)(A). (The Assad memo, referenced above, discussed a method for contractors to demonstrate implementation or "planned implementation" of the NIST SP 800-171 requirements by the Dec. 31, 2017 deadline using a "system security plan" and associated "plans of action" that describe, among other information, "how and when any unimplemented security requirements will be met." Assad memo at 2–3.)

Further, FAR Case 2017-016 indicates that a "technology team" was tasked with drafting a proposed FAR CUI rule. See "Open FAR Cases as of July 6, 2018" at 4, available at *www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf*. NIST SP 800-171 states that the clause "will apply the requirements contained in the federal CUI regulation and [SP] 800-171 to contractors," and "will also address verification and compliance requirements for the security requirements in" SP 800-171. NIST SP 800-171, Rev. 1, at v. NIST SP 800-171 also states that the "approaches to federal oversight will be determined through the uniform CUI FAR clause, future understandings, and any agreements between federal agencies and their nonfederal information-sharing partners." Id. at 16. The fact that companies are still working hard to understand and implement regulations that effectively constitute a new (and growing) area of federal procurement law is yet another reason for the Government to engage cooperatively with the contracting community—and avoid unreasonably severe remedies and sanctions—in overseeing these regulations. (One commenter stated earlier this year that "[w]hile no silver bullet exists for the problems of cybersecurity, the U.S. Government should refrain from shooting the private sector in the foot with new regulations and focus on strengthening the security of its own information." Walters, "Federal Cyber Breaches in 2017," The Heritage Foundation (Jan. 3, 2018), available at *www.heritage.org/cybersecurity/report/federal-cyber-breaches-2017*.)

The Government Should Look to Publications Discussing Cybersecurity of Government Information Systems as Guidance for Overseeing Cybersecurity Procurement Regulations: The Government has issued publications that, in discussing Government cybersecurity compliance, offer sound guidance that the Government should consider as it oversees contractor cybersecurity compliance. For example, NIST SP 800-39, "Managing Information Security Risk Organization, Mission, and Information System View," is the "flagship document in the series of information security standards and guidelines developed by NIST in response to FISMA." NIST SP 800-39 at 3 (March 2011), available at *nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf*. That publication states that when assessing federal agency compliance with NIST special publications, IGs, evaluators, auditors and assessors consider the *intent* of the security principles articulated in the specific guidance document and how agencies applied the guidance in the *context* of their mission/business responsibilities, operational environment and unique organizational conditions. Id. at iv n.3. That publication also states that the "ability of organizations to provide strategic information security investments is limited. Where the desired strategic investment funding or strategic resources are not available to address specific needs, organizations may be forced to make compromises." Id. at 16.

Also, NIST SP 800-171 notes that agencies using federal systems to process, store or transmit CUI must comply with NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations." NIST SP 800-171, Rev. 1, at 2–3. The NIST SP 800-53 security controls are designed to facilitate compliance with applicable federal laws, executive orders, directives, policies, regulations, standards and guidance—"[c]ompliance is *not* about adhering to static checklists or generating unnecessary FISMA reporting paperwork." Instead, compliance necessitates organizations executing due diligence with respect to information security and risk management, including using all appropriate information as part of an organization-wide risk management program to effectively use "the tailoring guidance and inherent flexibility in NIST publications so that the selected security controls documented in ... security plans meet the mission and business requirements of organizations." NIST SP 800-53, Rev. 4, at x (April 2013), available at *nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf*.

Further, the requirements of OMB Circular A-130, "Managing Information as a Strategic Resource," apply to the information resources management activities of all federal agencies. OMB Circular A-130, at 3 (July 28, 2016), available at *www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf*. In 2016, OMB revised the circular to reflect changes in law and advances in technology. In issuing the re-

vised circular, OMB stated, "Importantly, [the circular] represents a shift from viewing security and privacy requirements as compliance exercises to understanding security and privacy as crucial elements of a comprehensive, strategic, and continuous risk-based program at Federal agencies." 81 Fed. Reg. 49689 (July 28, 2016); see also Military Technology Transfer: Threats, Impacts, and Solutions for the Department of Defense: Hearing Before the H. Armed Services Comm. 115th Cong. (2018) (DOD joint testimony), available at *docs.house.gov/meetings/AS/AS00/20180621/108468/HHRG-115-AS00-Wstate-BingenK-20180621.pdf* ("[T]he Department is implementing a more holistic approach to industrial and information security. We are transitioning from a compliance, checklist-based National Industrial Security Program (NISP) to a risk-based approach informed by the threat and DoD technology priorities.").

Consistent with these principles, the Government should not adopt a rigid approach when assessing contractor efforts to comply with the multitude of cybersecurity requirements.

Conclusion—There are other important reasons why the Government should exercise caution before deploying harsh tactics when enforcing cybersecurity regulations, including the fact that it would further discourage commercial companies from doing business with the Government. The Government should recognize that it has initiated a significant expansion of procurement law that requires contractors and subcontractors to digest and comply with many complicated rules necessitating the use of IT professionals with specific skills. The difficulties involved in following these rules are evidenced in part by the Government's inability to meet similar cybersecurity standards covering agency information systems.

Rash and heavy-handed enforcement will be counterproductive. Among other consequences of such enforcement, contractors may be less willing to engage in a full-and-open dialogue with the Government about cybersecurity issues and problems that could benefit other contractors, as well as the Government's own information systems. Before lowering the hammer, the Government should keep in mind the foregoing facts—including the vast problems with its own information systems as evidenced in the recent OMB report and other Government publications.

As noted in Part I, asking the Government to consider the factors discussed in this Feature Comment when deciding to use one or more of the weapons in its enforcement arsenal is not asking the Government to forgo compliance with contract requirements. Indeed, if the Government really wants full compliance with cybersecurity regulations, it should adopt an approach that resembles the "partnering" approach championed for years by the Army Corps of Engineers. That approach is a way to reduce confrontations on a contract and build a collaborative project-focused team, and involves, among other factors, open communication and active listening. Partnering "is not a waiver of a party's contractual rights and responsibilities—it is a recognition and respect of those rights and responsibilities *and a willingness to work together to help all stakeholders fulfill them*" (emphasis added). See Army Corps of Engineers, Engineering and Construction Bulletin No. 2017-14, "Importance of Partnering to Military Programs and Civil Works Projects and Programs" at 1 (June 16, 2017), available at *www.wbdg.org/ffc/dod/engineering-and-construction-bulletins-ecb/ecb-2017-14*. Moreover, "[i]t is in the Government's best interest and it is consistent with the Government's implicit duty to act in a fair and reasonable manner." Id.

As the U.S. Court of Appeals for the Federal Circuit has held, the Government 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. Successful implementation of the cybersecurity regulations, including full compliance by contractors, will depend in no small part on Government cooperation with individual contractors.

✦

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. ***The author would like to thank Ray Monroe, a principal at Miles & Stockbridge, for his thoughts and comments on this Feature Comment.*** ***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.***

