THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 61, No. 29 **August 7, 2019**

Focus

¶ 224

FEATURE COMMENT: Guerrillas Of The NIST: DOD Re-attacks Supply Chain And Contractor Cybersecurity (Part I)

"Guerrilla war is a kind of war waged by the few but dependent on the support of the many."
Sir Basil Liddell Hart
Foreword to GUERRILLA WARFARE
by Mao Tse Tung and Che Guevara (1961)

While the Department of Defense's (DOD) recent, and renewed, focus on cybersecurity may not constitute "war" per se, the agency appears to have little problem littering the regulatory battlefield with rumors of an impending "shock and awe" strike. Like the actions taken by Nathanael Greene or Francis Marion, DOD's current efforts to address cybersecurity are, at the very least, disorienting and unconventional. Unfortunately, this does not help federal contractors. Cybersecurity is the three-ton, rainbow-colored elephant sitting atop every federal contractor's dining room table on Thanksgiving Day. It is, thus an "issue"—and one that is impossible to ignore. While some contractors may liken DOD's continuing promulgation of cybersecurity rules and regulations to just another screed from "Drunk Uncle" Sam, the sobering reality is that compliance with these requirements is absolutely critical to the avoidance of catastrophic liability. As such, many in the federal procurement community are now in the untenable position of deciding how—or when—to proceed in securing Controlled Unclassified Information (CUI) and, specifically, Covered Defense Information (CDI) being received or generated as part of contract performance. DOD's irregular warfare against cyber threats also has the unintended effect of disorienting requiring activities and contracting officers still struggling properly to identify CUI and CDI to contractors in the absence of clear guidance. Suffice it to say, it's a jungle out there and—in the middle of all of this turmoil—a little conventionality may be helpful. This Feature Comment will attempt to impose some clarity and calm on much of the chaos that has been emanating from DOD in recent months.

Over the course of the past eight years, since Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, was first issued in draft form in 2011, DOD has been hard at work grappling with the challenge of ensuring that the data it provides to its contractors remain secure and, if not secure, that the department knows when there has been a security lapse. Yet despite its efforts, a July 2019 DOD Office of Inspector General report reveals that "DoD contractors did not consistently implement DoD-mandated system security controls for safeguarding Defense information." See *Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems*, Report No. DODIG-2019-105, July 23, 2019. Moreover, beyond revealing contractors' shortcomings, the report identified that DOD contracting offices and requiring activities failed to create processes or procedures to:

- verify that contractors' networks and systems met National Institute of Standards and Technology [NIST] security requirements before contract award;
- notify contractors of the specific CUI category related to the contract requirements;
- determine whether contractors access, maintain, or develop CUI to meet contractual requirements;
- mark documents that contained CUI and notify contractors when CUI was exchanged between DoD agencies and the contractor; and

- verify that contractors implemented minimum security controls for protecting CUI.

Id. Perhaps more problematic, the report highlighted that these same components "did not always know which contracts required contractors to maintain CUI because the DoD did not implement processes and procedures to track which contractors maintain CUI … [and] inconsistently tracked which contractors maintain CUI on their networks and systems." Id. The collective effect of these systemic failures, the report concludes, is the ineluctable truth that the "DoD is at greater risk of its CUI being compromised by cyberattacks from malicious actors who will target DoD contractors." Id. As DOD grapples with these shortcomings, the agency has undertaken a variety of initiatives designed to address cybersecurity concerns that, in combination, are sure to spawn confusion while increasing contractor costs across the Defense Industrial Base.

Initiative #1 – Modernizing the Aging NIST Foundation—First, NIST issued a fairly routine change to the underlying set of standards meant to ensure that CDI is safeguarded. In this regard, NIST issued a draft release of Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, ***Revision 2.*** In the draft, which is largely editorial in nature, NIST promised that Revision 5 to SP 800-53, Security and Privacy Controls for Information Systems and Organizations, is forthcoming and will change its catalog of security controls leading to a subsequent "comprehensive update" to NIST SP 800-171 with its ***Revision 3***. But there are key elements that did, in fact, change of which contractors should take note and which are described below. The bottom line is that the rulebook is changing—a lot—and all in the shadows of two new NIST publications attempting to facilitate the use of the 800-171 requirements: (1) NIST SP 800-171***A***, Assessing Security Requirements for Controlled Unclassified Information, issued on June 13, 2018, and (2) a draft of NIST SP 800-171***B***, Enhanced Security Requirements for Critical Programs and High Value Assets. Issued on June 19, 2019, the draft NIST SP 800-171***B*** contains 33 enhancements to the 800-171 security requirements and is intended to protect CUI from advanced persistent threats (APTs). Just when contractors may have thought they had cybersecurity "on lock," more change is inbound.

Initiative #2 – DCMA Gets More Involved—The second broad action DOD has initiated will be arriving via the Defense Contract Management Agency (DCMA). As noted in a Jan. 21, 2019 memorandum issued by Undersecretary of Defense for Acquisition and Sustainment Ellen Lord, DCMA has been tasked to "leverage its review of a contractor's purchasing system in accordance with DFARS Clause 252.244-7001" to "validate, for contracts for which they provide contract administration and oversight, contractor compliance with the requirements of DFARS clause 252.204-7012" and NIST SP 800-171 for contractors and their respective "Tier 1 Level Suppliers." See Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review, available at *www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19 TAB A USD(AS) Signed Memo.pdf*. Shortly thereafter, DCMA updated its Contractor Purchasing System Review (CPSR) Guidebook by incorporating this mandate into its "Supply Chain Management Process," citing "[s]afeguarding DoD covered defense information [a]s a critical aspect of [Supply Chain Management]." See Contractor Purchasing System Review (CPSR) Guidebook, Appendix 24, February 26, 2019 (revised on June 14, 2019). Beyond the self-attestation contemplated under DFARS 252.204-7012 and the assessment provided by NIST SP 800-171A, the new role assumed by DCMA will empower its auditors to target and identify deficiencies with contractor (i) efforts to safeguard CDI, (ii) reporting of cyber incidents, and (iii) management of cybersecurity requirements through the entire supply chain. This is not a welcome development. As many contractors know all too well, an adverse finding by a DCMA auditor conducting a purchasing system review may lead to a determination that a "significant deficiency" exists in that system, and the contracting officer, in turn, may initiate monetary withholdings against the contractor. See, e.g., DFARS 252.242-7005(b), (d), (e).

Initiative #3 – A Uniform Certification Standard—Third, the most recent DOD cybersecurity initiative is the soft unveiling of its Cybersecurity Maturity Model Certification (CMMC) program. Employing a quaint, whistle-stop reveal of the program's intent and construction, DOD is allowing the CMMC to grow, like a rumor, with every new stop. Presently, the fairly unpopulated DOD website addressing the program (*www.acq.osd.mil/cmmc/*) notes that DOD is working with "DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDC), and industry to develop the Cybersecurity Maturity Model Certification." Notably, the website does not define exactly what a "Cybersecurity Maturity Model

Certification" actually is. In lieu of a definition, we are told that the CMMC's intentions are to:

- "review and combine various cybersecurity standards and best practices and map these controls and processes across several maturity levels";
- "build[ ] upon existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component with respect to cybersecurity requirements";
- "be cost-effective and affordable for small businesses"; and
- certify "independent 3rd party organizations to conduct audits and inform risk."

See *www.acq.osd.mil/cmmc/index.html*. PowerPoint slides provided at DOD's tour provide little additional insight, but new content and details appear to emerge in every town in which the train stops. While the laudable intent and rationale of the CMMC is to provide a workable and collaborative solution to CUI/CDI cybersecurity, the manner and timeline in which it is planned, the inclusion of new standards and best practices, along with DOD's tacit avoidance of formal changes to the FAR and DFARS or any written guidance, may end up causing more doubt and indecision by the Government and contractors alike.

In the pages that follow, we will examine each of these initiatives and will provide unified insight as to how they intersect and impact contractors' cybersecurity compliance efforts. We'll conclude with key takeaways designed to ensure that federal contractors are properly prepared to address the regulations that are sure to be the end result of DOD's current machinations.

NIST Updates, Revisions and Drafts—In the cybersecurity arena, NIST continues to move the dialogue forward with DOD contractors. Its efforts are creating a useable framework and guidance against which contractors are able to assess and measure their efforts against Government demands. That is not to say that the effort is easy—or inexpensive—but it is workable for those that take the time and expend the capital to do it. And, as we have been warning for years, the alternative—or the perceived alternative—can be far more expensive. See, e.g., *U.S. ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240, 1246 (E.D. Cal. 2019) (denying motion to dismiss the False Claims Act allegations raised by the contractor's former director of cyber security compliance and controls that his employer "misrepresented … to the government the extent to which it had equipment required by the regulations, instituted required security controls, and possessed necessary firewalls" in violation of DFARS requirements). The SPs and related guidance provide ample tools for federal contractors to ensure that Government safeguarding requirements are met.

NIST SP 800-171 Revision 2 and, Coming Soon, Revision 3: Arriving this summer with little fanfare was the draft release for comment of NIST SP 800-171, Revision 2. The purpose of its release was largely academic and, as recognized in its papers, intended to provide only "minor editorial changes in Chapter One, Chapter Two, and the Glossary, Acronyms, and list of References. There are no changes to the basic and derived security requirements in Chapter Three." See NIST SP 800-171, Revision 2 (DRAFT), Notes to Reviewers. In addition to the edits for simplicity, the draft also attempted to enhance SP 800-171 readability by integrating the SP 800-53 derived "Discussion" sections, located previously in Appendix F of Revision 1, alongside each of the respective security requirements "to facilitate the implementation and assessment of the requirements." See NIST SP 800-171, Revision 2 (DRAFT), 2.2 Development of Security Requirements. While the change is little more than a cut and paste, the change does make SP 800-171, Revision 2 more user-friendly. The period for public comment, extended through Aug. 2, 2019, has closed, so the community will need to wait to see how these editorial changes were taken.

Confidentiality is Integrity. As intended, there are no changes to the basic or derived security requirements in Revision 2, meaning that the same 110 total security requirements to ensure the confidentiality of CUI under SP 800-171 remain unchanged in SP 800-171, Revision 2, but the revision does provide some clarity to preexisting areas of confusion. Perhaps most notable is that Revision 2 contains a more affirmative and direct declaration aligning data confidentiality efforts to the concept of data integrity. In this regard, Revision 2 states expressly that "[t]he security objectives of confidentiality and integrity are closely related since many of the underlying security mechanisms at the system level support both objectives. Therefore, the basic and derived security requirements in this publication provide protection from unauthorized disclosure and unauthorized modification of CUI." See NIST SP 800-171, Revision 2 (DRAFT), Chapter 3 at FN 19. Revision 1 of SP 800-171 was far less definitive about this connection, stating only that an organization's efforts to ensure data integrity "may have a significant, albeit indirect effect on the ability of an organization to protect the confidentiality of CUI." See NIST SP 800-171, Revision 1, at FN 18. Since the NIST SP

800-171 Cautionary Note in both revisions still highlights that "[i]n addition to the security objective of confidentiality, the objectives of integrity and availability remain a high priority for organizations that are concerned with establishing and maintaining a comprehensive information security program," it is useful to see that NIST has now explicitly endorsed the nexus between safeguarding confidentiality and ensuring data integrity. Although data availability, or "[e]nsuring timely and reliable access to and use of information," still remains a necessary requirement for contractors outside the purview of NIST SP 800-171, this clarification linking data confidentiality and data integrity should assist contractors in ensuring proposed information security efforts are meeting the Government's needs.

System Security Plan Expansion. Another edit that may go unnoticed but which warrants examination is Revision 2's expectation that a nonfederal organization's required System Security Plan (SSP) is expected to "address known and anticipated threats." NIST SP 800-171, Revision 2 (DRAFT), Chapter 3. Beyond a simple edit, this is a significant—albeit warranted—addition that is not addressed specifically in Revision 2 or the current CUI SSP Template provided in conjunction with NIST SP 800-171 (available at *csrc.nist.gov/publications/detail/sp/800-171/rev-1/final*). As required by Security Requirement 3.12.4, the SSP is intended simply to describe "the system boundary; the operational environment; how the security requirements are implemented; and the relationships with or connections to other systems." NIST SP 800-171, Revision 1, Chapter 3. While these same descriptors remain in Revision 2, the inclusion of protection against ***threats*** into the SSP makes for a marked change with the SSP becoming more operational and, arguably, far more proprietary and sensitive. Moreover, the inclusion of "known and anticipated threats" would appear to require a contractor to develop a threat modeling capability that goes far beyond the kind of risk assessment originally indicated in prior versions of SP 800-171. This change may even hint at the security enhancements found in the draft of SP 800-171B as described below. Should this "minor editorial change" survive into the formal release of Revision 2 or beyond, contractors will need to update their SSPs to ensure that system and data threats are understood, contemplated, and fully addressed through the operation of the SSP.

But Wait, There's More. While it is uncertain what form Revision 2 will take, NIST continues its efforts to evolve its security controls and requirements to keep pace with existing and future threats. To that end, Revision 2 promises the release of two new relevant revisions: the long-delayed Revision 5 of NIST SP 800-53, Security and Privacy Controls for Systems and Organizations, and a new Revision 3 of NIST SP 800-171. Revision 5 of NIST SP 800-53 has been in limbo since the close of public comments in September 2017—*nearly two years ago*. It is expected, however, to be released in its final form this summer (which is quickly drawing to a close) and to provide broadly consumable guidance on next-generation security and privacy controls. Following the modified security control families and privacy integration contemplated under NIST SP 800-53, Revision 5, the release of NIST SP 800-171, Revision 3 promises to bring with it updates to Chapter 3's basic and derived security requirements in the "comprehensive update." Stay tuned.

NIST SP 800-171A, Assessing Security Requirements for CUI: Released on June 13, 2018, SP 800-171A is intended to provide organizations—federal and nonfederal alike—with an assessment methodology to evaluate compliance with the security and data safeguarding requirements identified in NIST SP 800-171, Revision 1. It is uncertain whether or how SP 800-171A will be amended to address the changes in Revisions 2 or 3, but we suspect that such a change will be forthcoming if the changes are as "comprehensive" as promised. All told, SP 800-171A is intended to be used as a tool by organizations concerned that SP 800-171 security requirements controls may be too broad. Accordingly, SP 800-171A sets out to clarify those requirements by providing assessors with generalized, flexible and customizable assessment procedures for each of the 110 controls that must be met to comply with the requirement. In fact, the guidance readily states that "[t]he assessment procedures can be used to generate relevant evidence to determine if the security safeguards employed by organizations are implemented correctly, are operating as intended, and satisfy the CUI security requirements." See NIST SP 800-171A, Cautionary Note. The document goes on to identify itself as the "primary and authoritative source of guidance for organizations conducting" SP 800-171 assessments and a tool capable of generating "evidence to support the assertion that the [SP 800-171] security requirements have been satisfied." See NIST SP 800-171A, 1.1, Purpose and Applicability.

In addition, each assessment objective is intended to dovetail with a company's SSP and contains "procedures, methods, and objects" that companies can use to assess compliance with CUI security requirements.

These include methods such as examinations of policies and procedures, interviews with key personnel, and/or system testing. Purposefully malleable, SP 800-171A allows the assessing organization flexibility to determine the scope, and the assessment and doesn't include any commandments dictating the level of assurances required to meet each security requirement. Rather, the objectives are achieved by applying the assessment method(s) chosen to obtain a finding that the security requirement is "*satisfied* or *other than satisfied.*" See NIST SP 800-171A, Chapter 3, The Procedures.

As will become apparent in discussions regarding DCMA and the CMMC in Part II, the purpose, intent, and usefulness of SP 800-171A will become increasingly important for federal contractors moving forward. The assessments it provides are not intended solely for self-reflection; "[t]he assessment procedures and methods can be applied across a continuum of approaches—including self-assessments; independent, third-party assessments; and assessments conducted by sponsoring organizations (e.g., government agencies). Such approaches may be specified in contracts or in agreements by participating parties." See NIST SP 800-171A, Cautionary Note.

As reflected in the DOD IG's July 2019 report, some contractors may benefit from the use of SP 800-171A. The report highlighted that the contractors examined, although small in number, were found to have deficiencies related to:

- using multifactor authentication;
- enforcing the use of strong passwords;
- identifying network and system vulnerabilities;
- mitigating network and system vulnerabilities;
- protecting CUI stored on removable media;
- overseeing network and boundary protection services provided by a third-party company;
- documenting and tracking cybersecurity incidents;
- configuring user accounts to lock automatically after extended periods and unsuccessful logon attempts;
- implementing physical security controls;
- creating and reviewing system activity reports; and
- granting system access based on the user's assigned duties.

Id. Notably, the DOD IG Audit's Scope and Methodology section indicated that the performance audit it undertook occurred from June 2018 through May 2019. However, the report makes no mention of using NIST SP 800-171A despite the SP being newly released in June of 2018. Despite the report's silence in this respect, DOD contractors should use the criteria set forth in NIST SP 800-171A when conducting assessments and should digest the results in advance of any formal cybersecurity audits.

NIST SP 800-171B, Enhanced Security Requirements for Critical Programs and High Value Assets: Sometimes, everything old is surely new again. As one may recall, on June 29, 2011—just over eight years ago—DOD started a new era of contractor cybersecurity when it first proposed amending the DFARS "to add a new subpart and associated contract clauses to address requirements for safeguarding unclassified DoD information." See 76 Fed. Reg. 38,089 (June 29, 2011). The proposed changes were intended to fill the then-existing gaps associated with implementing "adequate security measures to safeguard unclassified DoD information within contractor information systems from unauthorized access and disclosure, and to prescribe reporting to DoD with regard to certain cyber intrusion events that affect DoD information resident on or transiting through contractor unclassified information systems." Id. To accomplish this task, two clauses were contemplated, one for "Basic Safeguarding of Unclassified DoD Information," DFARS 252.204-70XX and one for "Enhanced Safeguarding of Unclassified DoD Information" DFARS 252.204-70YY. Id. While the two-tiered effort was ultimately abandoned in the DFARS, NIST appears to recognize that not all data—or Government programs—are created equally.

Enter the draft of NIST SP 800-171B, Enhanced Security Requirements for Critical Programs and High Value Assets, developed as a supplement to NIST SP 800-171, offering additional enhanced recommendations for protecting CUI in nonfederal systems and organizations where that information runs a higher-than-usual risk of exposure. Recognizing the threat imposed by sophisticated adversaries (e.g., the APT), the enhancements are intended to address CUI resident in critical programs or high-value assets which may increase the likelihood of it being targeted. The supplement notes further that these "enhanced security requirements are only applicable for a nonfederal system or organization when *mandated* by a federal agency in a contract, grant, or other agreement." See NIST SP 800-171B, CUI Enhanced Security Requirements (emphasis in original).

For those mandated to employ the enhancements they will face the inclusion of 33 more security requirements built on top of the pre-existing (*and already being met by the contractor*) 110 SP 800-171

security requirements. The enhancements are added to 10 of the 14 800-171 security families, as follows:

NIST SP 800-171B Security Requirement Families with Enhancements

3.1 Access Control
3.2 Awareness and Training
3.4 Configuration Management
3.5 Identification and Authentication
3.6 Incident Response
3.9 Personnel Security
3.11 Risk Assessment
3.12 Security Assessment
3.13 System and Communications Protection
3.14 System and Information Integrity

The enhancements are focused on augmenting a new multidimensional, defense-in-depth protection strategy by focusing on: "(1) penetration resistant architecture; (2) damage limiting operations; and (3) designing for cyber resiliency and survivability." See NIST SP 800-171B, Notes to Reviewers. The enhancements are identified by a numbering scheme based on the numbering format from SP 800-171, but with the inclusion of a lowercase "e" to the end of the control (e.g., 3.1.1e, 3.2.1e, 3.11.3e, etc.).

While the effect of the NIST SP 800-171B enhancements seems to pave the road to the multi-level distinction being crafted with the CMMC, described in detail in Part II, there are four key efforts that contractors should take to develop the resiliency of their existing networks in the event they may aspire to hold data commensurate with high-value programs:

- First, be prepared to address and enrich the company's network control access. The enhanced controls demand advanced efforts related to personnel access and data governance—at all stages of data rest and transit.
- Second, the enhanced requirements mandate a certain amount of baselining so as to better recognize the presence of the APT in contractor systems. This will mean not only a good portion of data governance but also ensuring employees with access to CUI are trained and capable of identifying suspicious or curious activity.
- Third, resiliency is generally going to be defined by the ability of a company to bounce back in the presence of a threat or incident, as incident response measures are key to this effort. Coordinating on resiliency and incident response means that plans and policies need to be robust, personnel need to be trained and tested, and the contingency planning needs to be rock solid.
- Fourth, companies will need to be prepared to perform thorough risk assessments and analysis, and be prepared to respond and adjust to the issues those assessments identify. Although directed toward larger prime contractors, the enhanced directives emanating from SP 800-171B are achievable to those contractors wishing to proceed into the high-value CUI asset arena so long as that drive is accompanied by commitment and grit.

The updates to, and creation of, new NIST Special Publications is a significant change for federal contractors. Not only do these changes now add to contractors' existing data safeguarding obligations, but they also herald a new era of cybersecurity requirements applicable to contractor information systems. What will that new era look like? What new DOD schemes loom for Defense vendors and agencies? How will contractors adjust to the seismic shifts demanded of them if they hold CDI? Tune in next week as we conclude the harrowing tale of *Guerillas Of The NIST*, same *The Government Contractor* time, same *The Government Contractor* place.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Alexander W. Major *and* Franklin C. Turner, *partners in the Washington, DC, office of McCarter & English. Mr. Major and Mr. Turner are co-leaders of the McCarter & English Government Contracts & Export Controls Practice Group.