THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 61, No. 30 **August 14, 2019**

Focus

¶ 231

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

> *"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)

As we discussed in Part I, federal defense contractors now must comply with new cybersecurity requirements propounded by the National Institute of Standards and Technology (NIST). The new standards, NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, *Revision 2;* NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information, issued on June 13, 2018, and the draft of NIST SP 800-171B, Enhanced Security Requirements for Critical Programs and High Value Assets, all provided updates to the manner in which defense contractors hold or should hold covered defense information (CDI). More interestingly, however, was the sense that these new standards were leading to bigger changes in the cybersecurity landscape, and indeed they were.

Unsurprisingly, the revised requirements and procedures newly deployed by NIST appear to be aligned with Department of Defense efforts to augment its cybersecurity demands on federal contractors. Those efforts include DOD tasking the Defense Contract Management Agency (DCMA) to "leverage its review of a contractor's purchasing system in accordance with [Defense Federal Acquisition Regulation Supplement] 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. The tasking led DCMA to update its Contractor Purchasing System Review (CPSR) Guidebook, allowing its auditors to target and identify purported deficiencies with contractor (i) efforts to safeguard CDI, (ii) reporting of cyber incidents, and (iii) management of cybersecurity requirements through the entire supply chain. Meanwhile, as contractors and DCMA prepare for change, DOD quietly unveiled a new cybersecurity initiative called the Cybersecurity Maturity Model Certification (CMMC) program, intended as a comprehensive and coordinated standard for cybersecurity, bringing together existing Government and industry cybersecurity requirements in an effort to secure the DOD supply chain by curing existing cybersecurity shortcomings within the Defense Industrial Base.

In the paragraphs that follow, we conclude our "brief" examination of the shifting landscape in the DOD cybersecurity arena and provide contractors with guidance as to how best to weather those changes.

Bring on the Auditors! DCMA Cybersecurity and the Revised CPSR Guidebook—Perhaps one of the biggest areas of concern after spending many years and dollars attempting to comply with a dizzying array of shifting cybersecurity requirements is knowing that, eventually, someone will be grading contractors on their current effort. Well, that's now going to happen. On Jan. 21, 2019, Undersecretary of Defense for Acquisition and Sustainment Ellen Lord issued a memorandum entitled "Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review" and, in

so doing, tasked DCMA "to validate, for contracts for which they provide contract administration and oversight, contractor compliance with the requirements of DFARS clause 252.204-7012." Premised on DCMA's mission of reviewing contractor's purchasing systems in accordance with DFARS clause 252.244-7001, Contractor Purchasing System Administration, the agency has now been directed to:

- "Review Contractor procedures to ensure contractual DoD requirements for marking and distribution statements on DoD [controlled unclassified information] flow down appropriately to their Tier 1 Level Suppliers. [and]
- Review Contractor procedures to assess compliance of their Tier 1 Level Suppliers with DFARS Clause 252.204-7012 and NIST SP 800-171."

While the tasking aims DCMA resources at prime contractors, it should be noted that a key focus of the effort appears targeted at "Tier 1 Suppliers," a term which is at the center of each direction and which likely refers to the first-tier subcontractors in the supply chain. This is a key distinction, as DCMA's task doesn't appear to be a SP 800-171A-type assessment of the actual prime contractor. Rather, it appears to address that prime contractor's efforts and procedures of (1) flowing down clauses such as DFARS 252.204-7012 and (2) ensuring that the prime contractor has procedures in place to assess its subcontractors' ability to safeguard CUI. In effect, this is a rather limited charge imposed on DCMA.

First and foremost, the direction is odd because nothing in DFARS 252.204-7012 or its reference to NIST SP 800-171 directs or requires prime contractors to create specific cybersecurity procedures of any kind. To be sure, Appendix E to SP 800-171 specifically identifies the assumptions upon which the security requirements are based with Tables E1 through E17 addressing the "Tailoring Actions" taken for each security family of requirements and specifically calling out those controls found in NIST SP 800-53 that are "Not Directly Related To The Confidentiality Of CUI," identified as "NCO," and those controls that are "Expected To Be Routinely Satisfied By Nonfederal Organizations Without Specification," identified as "NFO." Even a cursory glance through all the tables reveals that the presence of basic plans, policies and procedures—with the obvious exception of the System Security Plan (SSP) under NIST SP 800-171—is deemed NFO and not affirmatively or expressly mandated under SP 800-171 or the requirements found elsewhere in DFARS 252.204-7012. Absent a specific contractual requirement that a prime contractor possess, create or maintain procedures to assess their subcontractor's ability to safeguard CUI, DCMA auditors may find very little legitimate footing to support any contractual action premised on such findings. That said, we suspect that a lack of legal or factual support will do little to deter DCMA auditors from assessing purported "deficiencies" in a prime contractor's purchasing system. This is not to suggest that the auditors are "bad" in any respect. It is simply to state our informed recognition that Government auditors often feel as though it is their *mission* to find fault with contractors. Unfortunately, if an auditor fulfills this quixotic mission and assesses a significant deficiency in a contractor's purchasing system, the contractor may face significant potential liability in the form of withholdings against due and owing contract payments—particularly if the contract being audited includes the clause at DFARS 252.242-7005, Contractor business systems. As many contractors know all too well, this broadly interpreted clause explicitly permits pecuniary withholdings if the Government determines that, inter alia, the contractor's purchasing system contains "a shortcoming … that materially affects the ability of officials of the Department of Defense to rely upon information produced by the system that is needed for management purposes." Id. at (b), (e).

Further limiting DCMA's charge is the fact that its review is premised on DFARS 252.244-7001, a clause that does not apply to all contracts or contractors. First, DFARS 252.244-7001 is a clause that is required in solicitations and contracts containing the clause at FAR 52.244-2, Subcontracts. Pursuant to FAR 44.204, Contract Clauses, FAR 52.244-2 and thus DFARS 252.244-7001 are to be inserted in cost-reimbursement contracts and certain letter, fixed-price, time-and-materials or labor-hour contracts that exceed the simplified acquisition threshold. See FAR 44.204(a)(1). Additional limitations are provided by DCMA's own guidance that states "[a] CPSR is conducted when a contractor's annual sales to the Government are expected to exceed $50M in a 12-month period." CPSR Guidebook at 5. Suffice it to say, while DCMA has received a portion of a mission related to cybersecurity, it is not an all-encompassing, broad-reaching charge granting it unfettered access to assess the security posture of defense contractors. This may well come as a surprise to DCMA.

With DCMA's mission in hand, it was not long until revisions were made to the CPSR Guide-

book emphasizing DFARS 252.204-7012 on supply chain management. The first iteration was issued on Feb. 26, 2019, and later revised on June 14, 2019. The guidebook is intended to provide "guidance and procedures to Government personnel for evaluating contractor purchasing systems and preparing the CPSR reports." See CPSR Guidebook at 1.1, Introduction. As directed by DOD, part and parcel to those reviews is an examination of a contractor's supply chain management process and, specifically, the efforts undertaken by contractors when DFARS 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, and/or DFARS 252.204-7012 are present in their contracts. Id. at Appendix 24, Supply Chain Management Process. In line with the Jan. 21, 2019 memorandum, if the clauses are "applicable," DCMA is to evaluate the contractor's purchasing system to assess whether:

> (a) The contractor's covered defense information flowdown procedures ensure that DoD marking and dissemination statements, contractual requirements on contract deliverables, and DoD government furnished information, that contains marking and dissemination requirements, flow down appropriately to their subcontractors.
>
> (b) The contractor's procedures assure subcontractor compliance with DFARS Clause 252.204-7012.

Id. Where the direction and requirements may seem fairly straightforward, the CPSR Guidebook then proceeds to take significant liberty with its directives.

At the outset, assuming that the CPSR assessment is properly taking place pursuant to the confines of DFARS 252.244-7001 as stated above, it is worth noting that some contractors may find it arguable in the first instance that either DFARS 252.204-7008 or -7012 is even applicable to their contract. While the clauses may, indeed, be present in the underlying contract, true applicability is only supposed to be present when CDI is present or is expected to be generated during the life of the contract. That may not be the case in some contracts. One of the key takeaways from the DOD inspector general July 23, 2019 Audit Report was that DOD component contracting agencies often failed to "determine whether contractors access, maintain or develop CUI to meet contractual requirements" and "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." See "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," Report No. DODIG-2019-105, July 23, 2019. Applicability matters—if a company believes that CDI is not resident or applicable to their contracts, it should resist DCMA's efforts to assess the company's ability to meet requirements that should not be imposed upon it in the first instance.

Further, if the clauses do apply, remember that the CPSR Guidebook sets out a rather limited evaluation focused on flowdown procedures and subcontractor compliance. As set out in the guidebook, both of these facets may be improperly broad and are worthy of discussion with DCMA before proceeding. First, in order to assess whether CDI is flowing down properly to subcontractors, the procurement analyst (PA) does not necessarily need to receive a demonstration of the contractor's "ability to safeguard covered defense information in accordance with DFARS 252.204-7012," as the guidebook would have a PA seek. See CPSR Guidebook at Appendix 24. Policies and procedures addressing the flowdown of CDI should suffice. Similarly, as the CPSR concern is focused on supply chain management, it seems beyond the scope of the CPSR to "validate that [the contractor's] covered defense information is properly marked in procurement files containing DFARS 252.204-7012 and be aware that no covered defense information should be present in procurement files where DFARS 252.204-7012 is not included." Id. Again, while there may be a nexus between a contractor's data safeguarding effort and its supply chain management, there is no express linkage between the two that would warrant allowing CPSR PAs broad access to information security systems and architectures.

A second concern with CPSR Guidebook Appendix 24 relates to the manner in which a contractor is supposed to "assure subcontractor compliance with DFARS Clause 252.204-7012." The evaluation of subcontractor cybersecurity assurances imposes an implied, extracontractual obligation on prime contractors that may be improper. When it comes to subcontractor requirements imposed by DFARS 252.204-7012, all that is required is that contractors flow down the clause to subcontractors "if the information required for subcontractor performance retains its identity as covered defense information." DFARS 252.204-7012(m)(1). Assessing contractors against an artificial prerequisite that must "assure" subcontractor compliance asks contractors to demand more authority than DFARS 252.204-7012 grants. That said, most prime contractors understand that they are in privity of contract with the Government and that their subcontractors are not. In simple

terms, that means that prime contractors are always going to be "on the hook"—i.e., wholly responsible—for the sins of their subcontractors.

Cybersecurity Maturity Model Certification: Hero or Horror?—Against the backdrop of guideline revisions and auditing missions, DOD decided it would be a good time to unveil a new cybersecurity certification standard for DOD contractors. Partnering with the Carnegie Mellon University Software Engineering Institute and the Johns Hopkins University Applied Physics Laboratory, DOD announced the establishment of the new CMMC certification standard intending to usher in the next phase of defense contractor compliance … at least we think it is. Notably, we have been writing about the CMMC since first hearing about it in June 2019 and, while we know the CMMC is actually inbound, unlike the tangible changes to NIST Special Publications and the revisions to the CPSR Guidebook, program specifics are scant and details are amorphous. In that way, its reveal has more of a campaign promise-like vision rather than an affirmative standard upon which to base costly business decisions. Nonetheless, we will take a swing at attempting to address the scope of the CMMC's current iteration (as of July 31, 2019).

What we know of so far is that the CMMC program is resolved to secure the DOD supply chain by curing existing cybersecurity shortcomings within the Defense Industrial Base (DIB). Recognizing the challenges it has in store for itself, DOD envisions the CMMC as an adaptable model capable of evolving with present and future cyber threats. To meet this threat, the certification intends to create a comprehensive cybersecurity standard for the DIB that goes beyond the confines of NIST. Presently, that standard aspires to marry the NIST SP 800-171 and NIST SP 800-53 requirements and controls with industry standards and initiatives culled from the DIB Sector Coordinating Council, the Aerospace Industries Association voluntary National Aerospace Standard on cybersecurity (AIA NAS 9933), and international efforts such as the United Kingdom's National Cybersecurity Centre's "Cyber Essentials" and the Australian Cyber Security Centre's Essential Eight Maturity Model. Additionally, the DOD travelling rumor mill has stated that the National Archives and Records Administration is currently revising the definitions of CUI and CDI. The end result, DOD hopes, will be a multi-level, adaptive, comprehensive cybersecurity standard capable of being met by the DIB that can properly protect CDI that will arrive absent of any changes to existing DFARS clauses.

Similar to the stance taken by NIST SP 800-171B, the multi-level standard recognizes that while all unclassified defense programs are created equal, some are *more* equal and will require additional security and attention. To accommodate this reality, the required CMMC level for a specific contract will be contained in sections L and M of requests for proposals, and will serve as the basis of a "go/no-go decision" by the awarding activity. As it is presently contemplated, there are to be five certification tiers aligned with the level of cybersecurity sophistication the DOD contractor is expected to have in order to hold the data:

- CMMC Level 1 corresponds to "basic cyber hygiene."
- CMMC Level 2 corresponds to "intermediate cyber level hygiene."
- CMMC Level 3 corresponds to "good cyber hygiene."
- CMMC Level 4 corresponds to "proactive."
- CMMC Level 5 corresponds to "advanced and progressive [security]."

What standard(s) applies to what level is really nothing more than a matter of conjecture at this point. Comments from DOD seem to indicate that meeting the requirements of NIST SP 800-171, Revision 1, would place a contractor at somewhere between Level 1 and Level 3, with Level 4 and Level 5 reserved for the more advanced control requirements contemplated in the draft NIST SP 800-171B (and maybe NIST SP 800-171, Revision 3). What may not be conjecture at this point is that all DOD contractors—regardless of presence of CDI—may be required to meet the CMMC Level 1 standard. If this rumor is ever solidified into an actual contractual requirement, this would be a *significant* change for DOD contractors who, until this point, may have been spared from the strictures of cybersecurity requirements if they were able to avoid touching CDI.

As the standard and level-setting are being established, DOD anticipates that the CMMC program will be overseen and maintained by a neutral third party, with some comments suggesting it would be a non-profit. Who, exactly, that third-party is or the full scope of their authority remains shrouded in mystery, but whoever it is, they will be empowered to develop and deploy a tool that can be used by other third-party cybersecurity certifiers to conduct audits, collect metrics and inform risk mitigation for the entire supply chain. What is more, those third parties are envisioned to, somehow, provide contractors with real-time, remote scoring of their cybersecurity mea-

sures. While details remain scant, we do understand that the third-party entities assessing contractors will likely be barred from providing cybersecurity compliance services to those contractors as well. Vendors will have to pick which side of the aisle they want to be on: service or audit.

While the magnitude of DOD's CMMC initiative is stunning, everyone can recognize that it is an important and logical next step. The fact that it has taken this long for DOD to recognize that it needs to take a more affirmative stance in protecting its data is alarming. But the real incredulity about this program is its intended timing. As presently planned the first iteration of the CMMC standard is expected to be released in January 2020 alongside training programs for certifiers. That's in less than five months. That, we believe, is extremely optimistic. Moreover, the current timing suggests that the CMMC will begin appearing in solicitations starting in the fall of 2020.

The CMMC, in word and effect, injects a lot of uncertainty into understanding the data safeguarding contractual requirements found in DOD contracts. For now, our advice to clients is simply, ignore the sideshow. Proceed with the requirements in the contract and abide by the requirements of DFARS 252.204-7012. Have SSPs in place that demonstrate, pursuant to NIST SP 800-171A, that the company is able or will be able to adequately secure CDI, as those terms are defined in the contract. Albeit with new technology and new regulations, we recommend following the age-old mantra spoken by Government contracts for ages: Do what it says in your contract.

Practical Guidance—When it comes to irregular and guerilla warfare, Sun Tzu counseled in *The Art of War*: "Be extremely subtle, even to the point of formlessness. Be extremely mysterious, even to the point of soundlessness. Thereby you can be the director of the opponent's fate." There is something to be said about cybersecurity efforts being subtle, quiet, even adaptive and fluid; however, DOD needs to recognize that is not the best way to provide the standards upon which multiple parties are to be assessed for contract award. In light of the persistent change inundating contractors attempting to protect their data from the bad guys and their processes from the good guys, we suggest the following:

- In the midst of the uncertain regulatory background against which DOD contractors will be assessed, it is imperative that DOD contractors invest the time and resources to confirm that they meet the basic data safeguarding requirements identified in NIST SP 800-171, as mandated by DFARS 252.204-7012. While compliance with NIST SP 800-171 is by no means a comprehensive cybersecurity "fix," it is what is required to be a minimally compliant defense contractor—if that is the company's goal.
- The role of the SSP is maturing and should remain a vital and living element of a contractor's business capture and development efforts. The SSP should remain up-to-date and should be revised to address anticipated threats.
- Contractors should ensure that any cybersecurity requirements that are "Partially Implemented" or "Not Implemented" are appropriately tracked and maintained in an existing Plan of Action and Milestones (POAM). In addition, companies should assiduously address the issues identified in their POAMs, particularly since DOD may seek to obtain and evaluate them before award.
- Companies should carefully assess internal policies and procedures to ensure that cybersecurity compliance is maintained throughout their respective supply chains. This will mitigate the risk of potential downstream liability emanating from a purchasing system audit.
- Conduct training sessions—at least on an annual basis—to ensure that employees understand evolving cybersecurity requirements and that they will comply with those dictates. In addition, contractors should ensure that the incident response plan (IRP) is periodically tested and that roles responsible for handling and reporting CDI breaches are assigned and employees are properly trained.
- The NIST SP 800-171, Revision 2, Cautionary Note explicitly warns contractors 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." This means that if a company is following NIST 800-171 to the letter and doing nothing else, an organization would have ensured the safeguarding of its data, managed to keep some data integral, but done nothing to ensure the "timely and reliable access to and use of information." In addition to addressing the NIST list of requirements, contractors should ensure that they and their suppliers have ready access to the CDI they have been

given.

- Ensure (a) that the company possesses an IRP on hand and (b) that it includes the necessary instructions related to responding to breaches of CDI data. DFARS 252.204-7012 includes specific requirements related to reporting capabilities, which must be documented in the IRP.
- In light of the evolving nature of third-party assessments by DCMA and the CMMC, NIST SP 800-171A assessments may be a helpful tool by which contractors can demonstrate—primarily to Government auditors—that they are compliant with cybersecurity compliance and that they have performed the required internal due diligence on their systems. Contractors should, thus, create procedures for internal audits and subcontractor monitoring that align with the security assessment requirements identified in NIST SP 800-171A. While such procedures do not necessarily need to mirror the supplement, they should align with NIST requirements and methodologies for instances when a contractor is asked to provide assurances of internal or supply chain DFARS or NIST compliance.
- When the CMMC joins us in earnest, carefully evaluate solicitations to determine whether the articulated CMMC threshold is appropriate for the acquisition at issue. If a company believes that the CMMC level required is unduly restrictive of competition or is otherwise improper, it should strongly consider filing a pre-award protest. In a post-award context, companies should be prepared to protest no-go determinations. If the DOD IG Audit Report is any indication, there is a good chance that future technical evaluations regarding cybersecurity requirements will be flawed in one or more respects.
- In consultation with legal counsel, be prepared to push back against Government overreach where warranted. Remember, cybersecurity is a two-way street, and the Government has obligations with which it must comply. In addition, the Government does not have unlimited authority to comb through a contractor's books and records in search of a problem.

✦

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