AN A.S. PRATT PUBLICATION
MARCH 2019
VOL. 5 • NO. 3

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

LexisNexis®

PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 5 **NUMBER 3** **MARCH 2019**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com
Outside the United States and Canada, please call . . . . . (973) 820-2000

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
Customer Service Website . . . . . http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (937) 247-0293

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt);
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

PRATT'S GOVERNMENT CONTRACTING LAW REPORT is published twelve times a year by Matthew Bender & Company, Inc. For subscription information and customer service, call 1-800-833-9844. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to government contractors, attorneys and law firms, in-house counsel, government lawyers, and senior business executives. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher. POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 630 Central Avenue, New Providence, NJ 07974.

DOD and Other Agencies Seek to Enhance Contractors' Cyber and Supply Chain Security

By Robert K. Huffman, Natasha G. Kohne, and Thomas P. McLish*

The Department of Defense and its component services and agencies are taking several independent steps to assess and enhance their cyber and supply chain security that will directly or indirectly affect contractors and subcontractors. This article summarizes these initiatives and states the authors' view that, despite the proposal and likely adoption of a comprehensive new Federal Acquisition Regulation cybersecurity clause, federal government contractors and subcontractors are likely to face multiple, overlapping, and possibly conflicting cybersecurity and supply chain requirements for some time to come.

The Department of Defense ("DOD") and its component services and agencies are taking several independent steps to assess and enhance their cyber and supply chain security that will directly or indirectly affect DOD contractors and subcontractors. Other federal agencies, including the Department of Homeland Security ("DHS"), Department of Commerce, and General Services Administration ("GSA"), are also considering or implementing measures to enhance cyber and supply chain security that will directly or indirectly affect government contractors and their supply chains. These initiatives will intensify scrutiny of government contractors and subcontractors, increase their cyber and supply chain security compliance requirements, and affect their ability to compete for, and win, government contracts. This article summarizes these initiatives and states our view that, despite the proposal and likely adoption of a comprehensive new Federal Acquisition Regulation ("FAR") cybersecurity clause, federal government contractors and subcontractors are likely to face multiple, overlapping, and possibly conflicting cybersecurity and supply chain requirements for some time to come.

THE KEY ACTIONS

- Secretary of Defense James Mattis established a Protecting Critical

* Robert K. Huffman (rhuffman@akingump.com) is a partner at Akin Gump Strauss Hauer & Feld LLP representing defense, health care, and other companies in contract matters and in disputes with the federal government and with other contractors. Natasha G. Kohne (nkohne@akingump.com) is a partner at the firm and a co-leader of its cybersecurity, privacy and data protection practice. Thomas P. McLish (tmclish@akingump.com) is a commercial litigation partner at the firm focusing on cases involving government contract disputes, including bid protests and matters involving allegations of fraud or false claims.

Technology Task Force to address cybersecurity and supply chain risk.

- The Navy set forth stringent new cybersecurity requirements for critical technologies and programs that go well beyond the requirements of DFARS 252.204-7012.
- DOD issued final guidance to requiring activities for evaluating contractor compliance with the NIST Special Publication (SP) 800-171 ("NIST 800-171") standards and for imposing additional safeguards.
- DOD is auditing its contractors' compliance with cybersecurity requirements.
- DOD is supporting measures such as software bill of materials ("BOMs") and blacklists to identify and remove high-risk suppliers from its supply chain.
- DOD and DHS are implementing a Memorandum of Understanding regarding their respective roles in safeguarding critical infrastructure.
- GSA proposed new cyber incident reporting and system access requirements for its contractors.
- TSA adopted a cybersecurity roadmap to guide its efforts to ensure aviation and other transportation system resilience.

BACKGROUND

Even though the dust has barely settled on DOD's imposition of "adequate security" requirements through implementation of the Defense Federal Acquisition Regulation Supplement ("DFARS")-7012 clause and the National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-171 standards, DOD and other federal agencies face growing pressures to do more to safeguard their own, and their contractors', cyber and supply chain security.[1] These pressures have grown due to recent adversarial nation-state attacks on DOD and contractor information systems, as well as official and press reports on supply chain vulnerability to such attacks. These reports include the September 2018 White House Report on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, an October 2018 Government Accountability Office ("GAO") Report that was critical of DOD weapons systems cybersecurity,[2] and various Bloomberg press articles reporting that Chinese intelligence

[1] For example, Section 1647 of the FY 2016 National Defense Authorization Act requires DOD to complete an evaluation of the cybersecurity vulnerabilities of each of its major weapons systems by December 31, 2019.

[2] On December 12, 2018, GAO also released testimony before the Subcommittees on Government Operations and Information Technology, Committee on Oversight and Govern-

services had directed subcontractors to implant malicious chips in Supermicro server motherboards that were allegedly incorporated into the information systems of 30 large U.S. firms, including several contractors.

Even before these reports, DOD had announced a new Cybersecurity Strategy and begun an initiative focused on industry delivery of capabilities, services, technologies, and weapons systems uncompromised by adversaries. As part of this initiative, MITRE Corporation issued a report in August 2018 titled "Delivered Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," in which it recommended numerous enhancements for contractors' systems against hardware and software risks, including, most notably, making security the "fourth pillar" of acquisition planning in addition to cost, schedule, and performance.

Most recently, on December 14, 2018, the *Wall Street Journal* reported that Chinese hackers breached sensitive Navy data on contractor and research systems, leading Navy Secretary Spencer to order a classified review that validated the Navy's concerns and laid the groundwork for a response.[3] The *Wall Street Journal* article reported that Mr. Spencer's review comes as DOD "has struggled to steer its bureaucracy to more thorough digital security practices and give incentives to its subcontractors to safeguard themselves," and that "senior Pentagon leaders view the military's acquisition process as inadequately structured to hold contractors and subcontractors accountable for cybersecurity."[4]

These reports, and the threats described therein, provide the context for the actions described below.

SECRETARY MATTIS ESTABLISHES THE PROTECTING CRITICAL TECHNOLOGY TASK FORCE

On October 24, 2018, Secretary Mattis issued a memorandum[5] establishing the Protecting Critical Technology Task Force ("PCTTF"). The PCTTF is a cross-functional and cross-service task force that will work to protect "classified

---

ment Reform, House of Representatives. *See* https://www.gao.gov/products/GAO-19-275T. In the testimony, GAO concluded "federal agencies have taken steps to improve the management of information technology (IT) acquisitions and operations and ensure federal cybersecurity through a series of initiatives," but "significant actions remain to be completed."

[3] Gordon Lubold and Dustin Volz, *Chinese Hackers Breach U.S. Navy Contractors*, Wall Street J. (Dec. 14, 2018), https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401.

[4] *Id.*

[5] Billy Mitchell, *Mattis establishes DOD task force to protect critical tech, information*, FedScoop (Nov. 1, 2018), https://www.fedscoop.com/classified-information-protection-pentagon-task-force/

information, controlled unclassified information, and key data." To do so, Mattis directed the PCTTF to start with two separate "sprints" of 30 and 90 days to address basic cybersecurity problems. At the same time, the PCTTF will address "broader systemic issues." It is likely that many of these issues will include concerns over whether the current cybersecurity requirements in government contracts are robust enough to meet the challenges of modern technology supply chains, in particular, their vulnerability to unauthorized hardware and software injections in or by certain adversarial countries and entities.

Air Force Major General Thomas Murphy, who previously served as deputy director of command, control, communications, computers and cybersecurity for the Air Force Joint Staff, and, before that, as Vice Commander of Air Force Cyber, will lead the PCTTF. Staff for the PCTTF will come from the Secretaries of the Military Departments; Chairman of the Joint Chiefs of Staff; and various DOD agencies, including the Defense Intelligence Agency and the Defense Cyber Crime Center. The PCTTF will report to the Deputy Secretary of Defense, now being performed by David Norquist after the elevation of Patrick Shanahan to Acting Secretary of Defense.

The PCTTF may be planning to develop a method for certifying the cybersecurity compliance of DOD contractors. Once this compliance certification process is established, DOD would look to "change the NIST [800-171 standards] to be even more encompassing."[6]

THE NAVY DEMANDS ENHANCED CYBERSECURITY MEASURES FOR CERTAIN HIGH-RISK, CRITICAL TECHNOLOGIES AND PROGRAMS

The Navy recently adopted a proactive stance toward hardening its contractors' cybersecurity in response to reports of Chinese exfiltration of highly sensitive data from navy contractors and subcontractors.

On September 28, 2018, James Geurts, Assistant Secretary of the Navy for Research, Development, and Acquisition, issued a memorandum outlining the Navy's plan to impose enhanced cybersecurity measures on certain high-risk

---

[6] Aaron Boyd, *Pentagon Considers Cybersecurity Certification for Its Contractors*, NextGov.com, (Dec. 7, 2018), https://www.nextgov.com/cybersecurity/2018/12/pentagon-considers-cybersecurity-certification-its-contractors/153330/. With respect to changing the NIST 800-171 standards, Ron Ross of NIST announced at a NIST CUI requirement workshop on October 18, 2018, that NIST is preparing a revision to NIST 800-171 to address advanced persistent threats. According to Ross, this revised version would include enhanced security controls for highly sensitive information.

networks within the defense industrial base.[7] Effective immediately, the memorandum adds security measures beyond those applicable under DFARS-7012. This initiative follows other similar efforts by USTRANSCOM and the Missile Defense Agency ("MDA") to proactively engage contractors on cybersecurity, and may be followed by similar enhancement initiatives by the Army and Air Force.[8]

The additional measures identified in the Navy memorandum will apply to "current and future contracts, task or delivery orders" where designated Navy officials have determined that the "risk to a critical program and/or technology warrants it." Specifically, these contracts, task orders and delivery orders must include a Contract Data Requirement List ("CDRL") requiring the delivery and approval of a System Security Plan ("SSP") that implements the security requirements in DFARS-7012. The CDRL must contain a requirement that permits the government to validate the information in the SSP "every three years, on an ad hoc basis, with no notice to the contractor, or upon replacement or rotation of the Government program manager."

The Navy memorandum prohibits program managers from approving SSPs that do not:

- Fully implement multifactor authentication and authorization of users in a manner that is auditable;
- Fully implement FIPS 140-2 validated encryption;
- Employ the principle of least privilege or "need to know;"
- Require the contractor to review user privileges in a manner that can be audited at least annually;
- Require monitoring and control of remote access sessions and include mechanisms to audit the sessions and methods; and
- Implement, at a minimum, all security requirements in NIST 800-171 (Rev. 1) standards 3.1 to 3.14 (or equivalents approved by the DOD CIO).

---

[7] In addition, on December 3, 2018, the Naval Air Systems Command posted a solicitation for F-35 Joint Program Office Sustainment Supply Chain Risk Management. The solicitation is for the production and maintenance of F-35 supply chain mapping and associated risk assessment. *See*, https://www.fbo.gov/index?s=opportunity&mode=form&id=22252d97a5a2dbd6e235e9c2b1dea85e&tab=c%20ore&_cview=1.

[8] *See*, Six Recent Government Supply Chain Risk and Cybersecurity Initiatives (Aug. 13, 2018), *available at* https://www.akingump.com/en/news-insights/six-recent-government-supply-chain-risk-and-cybersecurity.html.

The Navy memorandum also requires cyber incident reporting in addition to that required under DFARS-7012. It requires program managers to include in all applicable contracts a CDRL requiring "delivery of *all information* related to cyber incidents (as defined in [-7012]) to the Defense Cyber Crime Center within 15 days of a cyber incident." (Emphasis added.) The CDRL must also require "segregation of [Navy] CUI from contractor-owned information, when feasible," such as through logical, physical, or hybrid isolation, or other acceptable methods.

The memorandum also imposes certain requirements in contract statements of work that exceed those included in NIST 800-171, including:

- Encrypting of data at rest per NIST 800-53 controls SC-13 and SC-28;
- Permitting the Naval Criminal Investigative Service ("NCIS") to install network sensors on information systems and assets when intelligence indicates an actual or potential vulnerability; and
- Requiring contractors to "engage with NCIS industry efforts and consider related hardening recommendations" for critical programs and technologies.

The Navy memorandum requires program managers to work with their contracting officers on solicitations for future contracts to include a requirement for submission of the pertinent sections of the SSP "for evaluation as part of any competitive source selection or sole source proposal review."

Regarding current contracts, the memorandum requires program managers to provide the Assistant Secretary with the following information within 30 days:

- A summary of the methodology used to assess whether current contracts within the purview of the Assistant Secretary should employ the additional requirements in the memorandum;
- A list of the current contracts and upcoming efforts that will be subject to the additional requirements in the memorandum;
- A summary of the contracts considered that will not include the requirements of the memorandum.

Finally, the memorandum requires the PEOs and the Chief of Naval Research to provide the Assistant Secretary within 180 days with an update on current contracts subject to the additional requirements of the memorandum that have not yet been modified to incorporate them.

The Navy memorandum is part of a trend toward balkanization of cybersecurity requirements. Other DOD services and component branches

have imposed or are considering additional requirements beyond those imposed by the DFARS-7012 clause and/or additional measures to assess or evaluate contractors' compliance with the DFARS-7012 requirements. So far, DOD has not sought to harmonize or replace these additional requirements. *Bloomberg Defense News* recently reported statements by Under Secretary of Defense for Acquisition and Sustainment Ellen Lord to the effect that DOD had developed contract language imposing additional cyber and supply chain requirements, but officials within DOD have characterized that report as erroneous. In fact, as discussed in the next section, DOD's final guidelines for assessing contractor cyber compliance expressly contemplate that DOD requiring activities may impose additional cyber requirements through individual solicitations and contracts.

There may soon be a proposed FAR clause that would impose the NIST 800-171 standards—and possibly the additional, enhanced controls being developed by NIST in response to advanced persistent threats on the information systems of federal government contractors.[9] The Information Oversight Office of the National Archives and Records Administration stated that "this FAR rule is necessary to ensure uniform implementation of the requirement of the controlled unclassified information (CUI) program in contracts across the government, thereby avoiding potentially inconsistent agency-level action," and it estimates that this FAR clause will be proposed for comment in January 2019.[10] However, even if this FAR clause is proposed and adopted, it remains to be seen how effective it will be in displacing the various cybersecurity safeguarding and reporting requirements, including those in the DFARS–7012 clause itself, that various agencies and sub-agencies have imposed on contractors.

In recognition of this "increasingly complex cybersecurity ecosystem," the Aerospace Industries Association of America ("AIA") issued a new standard on December 13, 2018, titled "Critical Security Controls for Effective Capability in Cyber Defense" (NAS 9933).[11] This standard borrows heavily from the Center for Internet Security's Critical Security Controls ("CSC") and Exostar's Control Level to Capability Level Matrix, which are designed in part "to align the additional requirements industry is experiencing through the DOD

---

[9] *See supra* note 3.

[10] Off. of Info. and Reg. Affairs, Off. of Mgmt. and Budget, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201804&RIN=9000-AN56.

[11] Nat'l Aerospace Standard, *Critical Security Controls for Effective Capability in Cyber Defense*, Aerospace Indus. Assoc. (2018).

contracting process."[12] The new standard is intended "to provide industry partners an idea of where a company is on the path to security beyond the compliance-based FAR, DFARS, and NIST SP 800-171 controls and a way to measure a company's cybersecurity risks," in lieu of "different DOD organizations using different tools in the contracting process to assess a company's security across different contracts . . . ."[13] Interestingly, the AIA's new standard and its reliance on Exostar capability measurement tools comes at the same time that DCMA and MDA have partnered to develop new DOD-wide cybersecurity compliance measurement tools, at least one of which is based on Exostar tools.

DOD ISSUES FINAL GUIDANCE TO REQUIRING ACTIVITIES FOR EVALUATING CONTRACTOR COMPLIANCE WITH NIST 800-171 AND IMPOSING ENHANCED SAFEGUARDS

On November 8, 2018, Kim Herrington, the Acting Principal Director, Defense Pricing and Contracting, issued a memorandum titled "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting" ("November Memo").[14] The November Memo incorporates two final guidance documents that DOD Components are "strongly encouraged to implement": (i) DOD Guidance for Assessing Compliance of and Enhancing Protections for a Contractor's Internal Unclassified Information System ("Assessment Guidance");[15] and (ii) DOD Guidance for Reviewing System Security Plans and the NIST 800-171 Security Requirements Not Yet Implemented ("Review Guidance").[16]

---

[12] *Id.* at 5.

[13] *Id.*

[14] Off. of the Under Sec'y of Def.: Def. Pricing and Contracting, Guidance for Assessing Compliance and Enhancing Prots. Required by DFARS Clause 252.204-7012, Safeguarding Covered Def. Info. and Cyber Incident Reporting (Nov. 8, 2018), https://www.acq.osd.mil/dpap/pdi/cyber/docs/Guidance_for_Assessing_Compliance_and_Enhancing_Protections.pdf.

[15] *Assessing the State of a Contractor's Internal Information System in a Procurement Action* (Apr. 24, 2018), https://www.regulations.gov/document?D=DARS-2018-0023-0002. DOD made a draft of this guidance available for public comment in April 2018. In the November Memo, DOD states that it incorporated comments it received from the public into the final documents. It appears that DOD addressed some of the issues raised by comments to the April 2018 draft.

[16] DoD Guidance for Reviewing System Security Plans and the NIST SP 800-171 Security Requirements Not Yet Implemented (Nov. 6, 2018), https://www.acq.osd.mil/dpap/pdi/cyber/docs/DoD%20Guidance%20for%20Reviewing%20System%20Security%20Plans%20and%20the%20NIST%20SP%20800%2011-6-2018.pdf.

The Assessment Guidance provides direction to DOD Components regarding the inclusion of evaluation criteria in solicitations and in contracts for assessing contractor compliance with NIST 800-171 and for imposing requirements that go beyond that standard. The Assessment Guidance references NIST 800-171A, which provides a framework for assessing compliance with NIST 800-171. It has three key objectives for pre- and post-award activities. For pre-award (solicitation and source selection) activities, the Assessment Guidance addresses (i) contractor self-attestation of implementation of NIST 800-171, (ii) imposing enhanced security controls beyond those in NIST 800-171, and (iii) approaches to using compliance with NIST 800-171 as an evaluation factor.

These approaches include:

- A "Go/ No Go" evaluation criterion/threshold based on the contractor's implementation of NIST 800-171 at the time of award, which would require delivery of the contractor's SSP and Plan of Action and Milestones ("POA&M") to evaluate against criteria included in Section M as to what would be an "acceptable" ("Go/No Go") threshold rating;
- Establishment of compliance with NIST 800-171 as a separate technical evaluation factor, which would also require delivery of the SSP and POA&M with a more detailed description of how compliance would be evaluated in Section M of solicitations;
- Conducting on-site assessments of the contractor's internal information systems in accordance with NIST 800-171A; and
- Requiring contractors to identify known Tier 1 suppliers and the contractors' plans for flowing down the requirements of DFARS-7012 and for assessing subcontractor compliance.

For post-award activities, the Assessment Guidance addresses three objectives:

- Delivery of SSPs and POA&Ms in accordance with a CDRL;
- On-site assessments of a contractor's covered defense information system; and
- Identification of covered defense information.

Each of these objectives would require corresponding provisions in Section C (Statement of Work) of the contract. The first objective would also require incorporation of the contractor's SSP (or parts thereof) and POA&M as part of the contract, which would make the SSP and POA&M contractually binding.

The Review Guidance provides direction to DOD Components on how to assess the risks and effects of not-yet-implemented NIST 800-171 security

controls.[17] It is divided into three columns: "NIST 800-171 Security Requirement," "Impact if this requirement is not yet Implemented" and "Implementation."[18] The first column merely lists the requirement. The second column "addresses the potential security consequences if a specific NIST 800-171 requirement is not implemented." The third column "addresses the approach a company might use to implement the NIST 800-171 security requirement, such as a policy, process, configuration, software or hardware change, or any combination of these." This column also provides "clarifying information . . . to address requirements which are often over-analyzed and/or misunderstood."

DOD AUDITS ITS AND ITS CONTRACTORS' CYBERSECURITY COMPLIANCE

Over the last several months, DOD officials have frequently emphasized the need—and the intent—to audit contractor cyber and supply chain security. Two specific, ongoing efforts toward this end include both a formal notice of DOD contractor cybersecurity audit by DOD's Office of the Inspector General ("OIG"), as well as less comprehensive assessments by the Defense Contract Management Agency ("DCMA").

While the full scope and related criteria of these audits and assessments remain unclear, recent comments by both contractors and government officials provide some insight on how the two differ and what contractors can expect on each front.

Since the DOD released its updated FAQs on DFARS clause 7012 and NIST 800-171 in April 2018,[19] industry has speculated on the exact scope and timing of enforcement, including which agency or office will lead that enforcement. Since then, various details have emerged about DCMA's efforts to assess contractor cybersecurity. Recent comments by officials tend to confirm, for example, that DCMA's role is currently focused on a company's SSP and POA&M, and that the agency is "not resourced" to fully evaluate SSPs and

---

[17] The Review Guidance should "not to be used to assess implemented security requirements, nor to compare or score a company's approach to implementing a security requirement."

[18] The April 2018 draft Review Guidance contained "Priority" and "DOD Value" columns that may have not been as clear as the final Review Guidance.

[19] R. K. Huffman, et al., *White Paper: Recent Dep't of Def. Guidance on Cybersecurity Requirements and Related Export Control Issues* (May 31, 2018), https://www.akingump.com/images/content/8/0/v2/80337/cybersecurity-white-paper-053118.pdf; *see also* Dep't of Def. Procurement Toolbox, *Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 [and] 239.76* (revised Apr. 2, 2018), https://dodprocurementtoolbox.com (follow "FAQs" hyperlink; then click "Cybersecurity FAQs"; then click "Cybersecurity FAQs Download").

implementation of underlying controls, among other substantive aspects of cybersecurity.[20] In order to close this assessment capability "gap," DCMA has partnered with MDA in a pilot program to develop alternative approaches for assessing a contractor's compliance with the NIST 800-171 controls and any enhanced controls that the services or other DOD components may impose. One of these approaches is reportedly based on tools developed by Exostar for measuring a company's cybersecurity capabilities.

By contrast, the DOD OIG's ongoing assessment of contractor cybersecurity may engage some contractors at a far more substantive level of cybersecurity compliance. Earlier in 2018, the DOD OIG announced its plan to audit defense contractors to determine "whether [they] have security controls in place to protect the DOD controlled unclassified information maintained on their systems and networks from internal and external cyber threats."[21] Though the specific scope and criteria involved have not been publicized, some contractors have indicated and expressed concern that the OIG's efforts go deeper than assessing implementation of SSPs and POA&Ms.[22] Indeed, there are reports that the DOD OIG audits go beyond assessing risks to CDI, and may extend to the adequacy of the contractor's safeguard controls for all CUI in its, and its subcontractors', possession.

Separately, the DOD OIG's recent audit of DOD's first full financial report included a cybersecurity dimension. In addition to finding material weaknesses or deficiencies in the financial/accounting systems of several DOD entities that prevented them from receiving a passing grade, the DOD OIG audit noted "systematic shortfalls in implementing cybersecurity measures to guard the data protection environment," including "internal control related items such as a need for increased managerial oversight, for an improved self-assessment program, for increased oversight capability, and for useful nuclear inspection reports."[23]

Most recently, at the Charleston Defense Contractors Defense Summit on December 6, 2018, DOD officials reportedly discussed DOD's desire to assess

---

[20] *See* Nat'l Inst. of Standards and Tech., *Controlled Unclassified Info. Sec. Requirements Workshop (Part 2)-NIST* (Oct. 18, 2018), https://www.nist.gov/news-events/events/2018/10/controlled-unclassified-information-security-requirements-workshop.

[21] Dep't. of Def. Office of the Inspector Gen., *Audit of the Prot. of DoD Info. Maintained on Contractor Systems and Networks (Project No. D2018-D000CR-0171.000)* (Jun. 22, 2018), https://media.defense.gov/2018/Jul/02/2001938018/-1/-1/1/D2018-D000CR-0171.000.PDF.

[22] *See* NIST CUI Workshop, *supra*.

[23] U.S. Dep't of Def., Agency Financial Report (2018), https://comptroller.defense.gov/Portals/45/Documents/afr/fy2018/DoD_FY18_Agency_Financial_Report.pdf%20.

and certify cybersecurity compliance. The officials provided few details, but hope to have a certification process in place within the next year.

DOD SUPPORTS MEASURES SUCH AS SOFTWARE BILLS OF MATERIALS AND BLACKLISTS TO IDENTIFY AND REMOVE RISKY SUPPLIERS FROM ITS SUPPLY CHAIN

DOD is increasingly focusing on identifying vulnerabilities in its supply chain and preventing their exploitation.[24] One of DOD's driving concerns is the risk that software that is produced or obtained from certain countries may be vulnerable to exploitation by foreign intelligence agencies and militaries.[25] Foreign companies are often vulnerable to foreign state influence, including requirements to provide foreign governments with access to physical or virtual security networks, or requirements to cooperate actively with foreign security services.[26] Hostile foreign parties may also more easily access physical storage or networks located in foreign countries. Additionally, certain foreign governments require companies seeking to sell their products in those countries to provide their source code for review by the countries' intelligence agencies.[27]

Identifying the origin of software and equipment is crucial to knowing what risks are potentially present, especially in critical systems. DOD recently instituted a pilot program to determine which companies are in the supply chain at all levels for military procurements.[28] Although Lockheed Martin has

---

[24] Ellen Nakashima, *Pentagon is rethinking its multibillion-dollar relationship with U.S. defense contractors to boost supply chain security*, Wash. Post (Aug. 13, 2018), https://www.washingtonpost.com/world/national-security/the-pentagon-is-rethinking-its-multibillion-dollar-relationship-with-us-defense-contractors-to-stress-supply-chain-security/2018/08/12/31d63a06-9a79-11e8-b60b-1c897f17e185_story.html. DOD's Defense Industrial Base hosts quarterly meetings to share best practices and threat information—contractors can join voluntarily. *See* Donald Heckman, Principal Director, Chief Information Officer, DOD, Cybersecurity in Large Organizations at NIST Cybersecurity Risk Management Conference (Nov. 7, 2018).

[25] Marcus Weisgerber & Patrick Tucker, *Pentagon Creates "Do Not Buy" List of Russian, Chinese Software*, Defense One (July 27, 2018), https://www.defenseone.com/threats/2018/07/pentagon-creates-do-not-buy-list-russian-chinese-software/150100/. Supporting this fear, on October 4, 2018, *Bloomberg Businessweek* reported that China had hidden microchips in motherboards sold by Supermicro to numerous U.S. companies. However, recent articles have reported that there is no evidence supporting the claims in the *Businessweek* article.

[26] Foreign Economic Espionage in Cyberspace, Nat'l Counterintelligence and Sec. Ctr. 14 (2018).

[27] *Id.*

[28] Justin Lynch, *Pentagon moves to secure supply chain from foreign hackers*, Fifth Domain (Oct. 21, 2018), https://www.fifthdomain.com/dod/2018/10/21/pentagon-moves-to-secure-supply-chain-from-foreign-hackers.

spoken generally about its involvement in the pilot program, further details of this program, such as its scope, findings, and other participants, remain unclear.[29]

DOD is also supporting efforts by Commerce and DHS to require or incentivize contractors to provide software BOMs that would allow the government to pinpoint and remediate cybersecurity risks posed by components that originate in countries or with firms that pose a threat to the United States.[30] However, while a BOM may be required under individual contracts, there remains no harmonized, integrated approach in the federal government regarding the necessity of a BOM, or indeed regarding sharing of information regarding risk assessments and supply chain threats.[31]

As part of its efforts to reduce the risk of integrating compromised software into its systems, DOD recently caused waves by suggesting that Undersecretary Lord had created a "do-not-buy" list of mostly Russian and Chinese software and equipment.[32] Under the reported do-not-buy list, defense contractors would not be permitted to purchase blacklisted products or contract with blacklisted companies under DOD contracts, but could potentially do so for unrelated work.[33] Other, more recent press reports suggest that this do-not-buy list does not, in fact, exist; in response to a Freedom of Information Act request for the list, DOD stated that no such records could be found, and that "the 'do not buy' list referenced by Undersecretary Lord was a misuse of the phrase 'do not buy.' "[34]

Although DOD's do-not-buy list may not exist, the federal government has "blacklisted" certain companies before due to cybersecurity concerns. Section

---

[29] *Id.*

[30] Scott Maucione, *DOD, Commerce consider requiring "ingredients list" of software to protect supply chain*, Fed. News Network (Oct. 23, 2018), https://federalnewsnetwork.com/defensemain/2018/10/dod-and-commerce-are-looking-into-requiring-ingredients-list-of-software-to-protect-supply-chain.

[31] *Id.*

[32] Roxana Tiron, *Pentagon's "Do Not Buy" List Targets Russian, Chinese Software*, Bloomberg (July 27, 2018), https://www.bloomberg.com/news/articles/2018-07-27/pentagon-s-do-not-buy-list-targets-russian-chinese-software.

[33] Nitish Singh, *Pentagon and Department of Defense Releases a Blacklist of Software Providers*, TechNadu (July 30, 2018), https://www.technadu.com/pentagon-department-of-defense-blacklistsoftware-providers/36857.

[34] Thomas Claburn, *We asked the US military for its "do not buy" list of Russian, Chinese gear. Surprise: It doesn't exist*, The Register (Nov. 16, 2018), https://www.theregister.co.uk/2018/11/16/dod_donotbuy_list.

889 of the National Defense Authorization Act ("NDAA") for Fiscal Year 2019 prohibited all federal agencies from procuring any equipment or services from Huawei Technologies Company or ZTE Corporation, and from contracting with any entity that uses component parts or services from the two companies.[35] Similarly, FAR 52.204-23 prohibits federal agencies and contractors from contracting at any level for hardware, software, or services developed or provided by Kaspersky Lab, a software company that was reportedly connected to Russian intelligence agencies, and it imposes a rapid reporting requirement on contractors that identify Kaspersky Lab in their supply chain.[36]

As part of its own focus on supply chain management, DHS has established the Information and Communications Technology ("ICT") Supply Chain Risk Management Task Force, a public-private partnership that is intended to examine and develop consensus recommendations for identifying, managing and reducing the supply chain risks to federal agencies and the global ICT supply chain.[37] Emile Monette of DHS preliminarily identified three "work-streams" for the task force: (i) an addition to the FAR that would require contractors to use "only 'authorized' equipment makers and sellers," (ii) "best practices for threat assessments around supply chains" and (iii) "creating 'qualified' bidders and manufacturers lists."[38] Although the DHS task force is not specifically focused on protecting the hardware and software that federal agencies use, another DHS official said that one of the task force's key goals is to help prevent agencies from buying technologies with security problems. DHS has also engaged the private sector with a formal Request for Information seeking information about industry's "capabilities" to conduct supply chain due diligence on ICT products and ICT-based services.[39]

On December 5, 2018, Robert Kolasky, head of DHS's National Risk Management Center and Director of DHS's newly renamed Cybersecurity and Infrastructure Security Agency, announced that he, himself, was replacing

---

[35] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a) (2018).

[36] FAR 52.204-23.

[37] Charlie Mitchell, *Tech-telecom task force leaders craft plans for DHS-led supply-chain initiative, eye "state of the art" report*, InsideCybersecurity.com (Nov. 9, 2018), https://insidecybersecurity.com/daily-news/tech-telecom-task-force-leaders-craft-plans-dhs-led-supply-chain-initiative-eye-%E2%80%98state.

[38] *Id.*

[39] *See* Cyber Supply Chain Risk Management, Solicitation Number: RNCC-18-60068 (Aug. 17, 2018) (updated Oct. 11, 2018), https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=c79780e7e36d25b1eef795b89261f589&_cview=0.

Monette as the government co-chair of the ICT Supply Chain Risk Management Task Force. Kolasky said that the change would allow better outreach to other government agencies because "in the government, rank and that sort of stuff matters, and I will use my relationships with other [agency] executives to make sure that they are engaged and remain engaged." Kolasky also stated that the task force would reexamine the workstreams preliminarily identified by Monette. In particular, Kolasky noted that "there are things we're going to do to push federal acquisition reform," but would consider whether these things "are rightly done through the task force or not."

In addition to the individual efforts by DOD and DHS, S. 3085, the Federal Acquisition Supply Chain Security Act of 2018,[40] would, if executed, provide exclusion authority to the Federal Acquisition Security Council.[41] The Council would have the authority to issue "exclusion orders" recommending the exclusion of goods or services from executive agency procurement and recommending the removal of articles from executive agency information systems.[42]

DOD AND DHS EXECUTE A MEMORANDUM OF UNDERSTANDING REGARDING THEIR RESPECTIVE ROLES IN SAFEGUARDING CRITICAL INFRASTRUCTURE

On November 14, 2018, a DHS official confirmed that DOD and DHS had established a memorandum of understanding regarding how the departments will work together on cybersecurity issues. The memorandum includes a new plan to identify the components of domestic critical infrastructure to prioritize for cyber protection. The memorandum "reflects the commitment of both departments in collaborating to improve the protection and defense of the U.S.

---

[40] On December 12, 2018, Cybersecurity and Infrastructure Security Agency Director Christopher Krebs recommended quick passage of S. 3085 in written congressional testimony.

[41] The Council consists of the Office of Management and Budget, the General Services Administration, DHS, the Office of the Director of National Intelligence, the Department of Justice, the Department of Commerce and "other executive agencies as determined by the Chairperson."

[42] Pursuant to 10 U.S.C. § 2339a, DOD currently has certain exclusion authority. As implemented through DFARS Subpart 239.73, the DOD may "[e]xclude a source that fails to meet qualification standards established in accordance with the requirements of 10 U.S.C. § 2319, for the purpose of reducing supply chain risk in the acquisition of covered systems"; and "[e]xclude a source that fails to achieve an acceptable rating with regard to an evaluation factor providing for the consideration of supply chain risk"; or "withhold consent for a contractor to subcontract with a particular source or direct a contractor for a covered system to exclude a particular source from consideration for a subcontract under the contract."

homeland from strategic cyber threats," according to Homeland Security Assistant Secretary Jeanette Manfra.[43]

This is not the first time that DOD and DHS have attempted to work together to combat cyber threats,[44] so we have to wait and see how the memorandum is actually implemented.

GSA PROPOSES CYBER INCIDENT REPORTING AND ACCESS REQUIREMENTS FOR ITS CONTRACTORS

GSA issued a proposal to amend the GSA Acquisition Regulation ("GSAR") to require contractors to report cyber incidents affecting the GSA.[45] The proposed GSAR clause would establish a time frame for reporting if the confidentiality, integrity or availability of information or information systems owned or managed by or on behalf of the U.S. government is potentially compromised.

The proposed GSAR clause would also describe GSA's (and ordering agencies') right to access contractor systems in the event of a cyber incident, require contractors to preserve an image of the breached system and ensure that contractor personnel receive training regarding the reporting of cybersecurity incidents. Further, GSA will protect any information reported by the contractor as required after a breach.

THE TRANSPORTATION SECURITY ADMINISTRATION ISSUES A "CYBERSECURITY ROADMAP" FOR THE AVIATION INDUSTRY AND OTHER TRANSPORTATION SECTORS

The Transportation Security Administration ("TSA") issued a "Cybersecurity Roadmap" on December 4, 2018, outlining how it intends to ensure the resilience of the transportation sector, which includes aviation (passenger and cargo), highway and water carriers, maritime, mass transit and passenger rail, pipelines, freight rail, and postal and shipping.[46] TSA's roadmap identifies six goals on which its cybersecurity efforts will be focused over the next five years:

---

[43] *Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of the Department of Defense & the Department of Homeland Security: Hearing Before the H. Subcomm. on Cybersecurity and Infrastructure Protection of the H. Comm. on Homeland Sec.*, (Nov. 14, 2018), https://www.dhs.gov/news/2018/11/14/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity (statement of Assistant Sec'y Jeanette Manfra).

[44] Cheryl Pellerin, *DOD, DHS Join Forces to Promote Cybersecurity*, U.S. Dep't of Def. (Oct. 13, 2010), http://archive.defense.gov/news/newsarticle.aspx?id=61264.

[45] Introduction to the Regulatory Plan and Unified Agenda of Federal Regulatory and Degregulatory Actions, Regulatory Info. Serv. Ctr., https://www.federalregister.gov/documents/2018/11/16/2018-24084/introduction-to-the-unified-agenda-of-federal-regulatory-and-deregulatory-actions-fall-2018.

[46] TSA Cybersecurity Roadmap 2018, Transp. Sec. Admin. (2018), https://www.tsa.gov/

- Assess and prioritize evolving cybersecurity risks to TSA and the transportation systems sector ("TSS");
- Protect TSA information systems;
- Protect TSS critical infrastructure;
- Respond effectively to cyber incidents;
- Strengthen the security and resilience of the cyber environment; and
- Improve management of TSA and TSS cybersecurity activities.

Regarding the goal of protecting TSS critical infrastructure, the roadmap states that TSA will engage TSS stakeholders on a regular basis "to evaluate their implementation of guidance and to determine their cybersecurity practices and to promote resilience to malicious cyber activity."[47] The roadmap further states that, "[i]f necessary, TSA will utilize its statutory and regulatory authorities to ensure the resilience of the TSS."[48]

CONCLUSION

Federal government contractors and subcontractors need to keep abreast of these initiatives and others that will likely follow given the evolving nature of cybersecurity and supply chain security threats and responses.

---

sites/default/files/documents/tsa_cybersecurity_roadmap.pdf.

[47] *Id.* at 10.

[48] *Id.*