GIVING THE CYBERSECURITY MATURITY MODEL CERTIFICATION TEETH: ENSURING COMPLIANCE IN CONTRACTOR SELF-CERTIFICATIONS

MAJOR THOMAS J. HOESMAN*

I. Introduction

In early 2018, the Chinese Ministry of State Security obtained 614 gigabytes of data from a contractor working for the Naval Undersea Warfare Center by compromising its unclassified electronic information storage systems.[1] The contents of the breach, while unclassified,[2] were sensitive enough that the Department of Defense (DoD) declined to disclose even the specific nature of the contract,[3] and the news outlet that broke the story agreed to withhold certain information it had uncovered because of its potential to "harm national security."[4] As noted at the time, "hundreds of mechanical and software systems [concerning undersea warfare] were compromised—a significant breach in a critical area of warfare that China has identified as a priority, both for building its own capabilities and challenging those of the United States."[5] This loss of non-public but unclassified information related to the contractor's project "deeply reduce[d] [the DoD's] level of comfort if [it] were in a close

* Judge Advocate, United States Air Force. Presently assigned as Acquisition Counsel, Air Force Materiel Command, Wright-Patterson Air Force Base, Ohio. LL.M., 2022, The Judge Advocate General's Legal Center and School, U.S. Army; J.D., 2015, University of Maryland Francis King Carey School of Law; B.A., 2012, St. Mary's College of Maryland. Previous assignments include Area Defense Counsel, Trial Defense Division, Vandenberg Space Force Base, California, 2019–2021; Chief of Administrative Law and Trial Counsel, 30th Space Wing, Vandenberg Air Force Base, 2016-2019. Member of the Bars of Maryland and the Supreme Court of the United States. This paper was submitted in partial completion of the Master of Laws requirements of the 70th Judge Advocate Officer Graduate Course.

[1] Ellen Nakashima & Paul Sonne, *China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare*, WASH. POST, (June 8, 2018; 3:04 PM), https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html.

[2] *See id.* (noting that the contents were not classified, although if aggregated "could be considered classified").

[3] *See id.* (disclosing only basic information concerning the breach without discussing the contractor or the specific purpose of the contractor's work).

[4] *Id.*

[5] *Id.*

undersea combat situation with China."[6] The breach was, unfortunately, not unprecedented. In recent years, as many as 44 percent of defense contractors have been the victim of successful cyber-attacks,[7] many at the hands of China and other adversaries.[8]

These breaches, and the theft of unclassified but sensitive information, are receiving significant attention. The DoD, in order to function, relies upon as many as 300,000 private companies and other entities to supply products and services.[9] These contractors[10] provide crucial support to the DoD's warfighting mission, and in doing so, are often entrusted with sensitive information to perform their requirements.[11] As illustrated above, adversaries have taken advantage of this access and engaged in highly effective, and often high-profile, efforts to obtain information from contractors' cybersecurity systems.[12] Multiple reports detailing widespread deficiencies in contractors' cybersecurity systems,[13] along with the DoD's failure to effectively monitor and identify those deficiencies (despite efforts to do so) have heightened concerns surrounding these attacks.[14]

To more effectively address these concerns, in 2019 the DoD released draft plans to transition to a framework it is calling the Cybersecurity

---

[6] *Id.*

[7] NAT'L DEF. INDUS. ASS'N, BEYOND OBFUSCATION: THE DEFENSE INDUSTRY'S POSITION WITHIN FEDERAL CYBERSECURITY POLICY 21 fig.15 (2019).

[8] *See* Editorial, *Contractors Are Giving Away America's Military Edge*, BLOOMBERG (Apr. 18, 2019, 2:36 PM), https://www.bloomberg.com/opinion/articles/2019-04-18/defense-data-breaches-pentagon-must-hold-contractors-accountable (identifying the actors behind several high-profile breaches of contractor systems).

[9] HEIDI PETERS, CONG. RSCH. SERV., R46643, DEFENSE ACQUISITIONS: DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION FRAMEWORK 1 (2020).

[10] The term "contractor," as used throughout this article, references "[a]ny individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the D[o]D to furnish services, supplies, or construction." 32 C.F.R. § 158.3 (2021).

[11] *See* INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2019-105, AUDIT OF PROTECTION OF DOD CONTROLLED UNCLASSIFIED INFORMATION ON CONTRACTOR-OWNED NETWORKS AND SYSTEMS 3 (23 July 2019) [hereinafter DOD IG ROI-CONTRACTOR-OWNED NETWORKS] (discussing the requirements for those contractors who are entrusted with controlled unclassified information).

[12] *See Contractors Are Giving Away America's Military Edge*, *supra* note 8 (describing several high-profile breaches of contractor systems).

[13] *See, e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (identifying significant cybersecurity deficiencies by every contractor evaluated).

[14] *See, e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 27-33 (noting that "[n]either DoD [c]omponent [c]ontracting [o]ffices [n]or DoD [r]equiring [a]ctivities [a]ssessed [c]ontractors' [a]ctions for [p]rotecting [i]nformation" despite requirements to do so).

Maturity Model Certification (CMMC).[15] Since then, the DoD has further refined its model with the release of the CMMC 1.0 framework,[16] an interim rule amending the Defense Federal Acquisition Regulation Supplement (DFARS),[17] and finally, the release of plans for the most current version of the CMMC framework, CMMC 2.0.[18] Under the updated version of the framework, the majority of contractors will self-certify that they have met cybersecurity requirements designed to keep their information systems secure,[19] which continues the DoD's reliance on contractors to review their own cybersecurity measures despite historical challenges associated with this approach.[20]

While the CMMC program is necessary to address glaring weaknesses in contractor cybersecurity,[21] the plan to require such a large group of contractors to self-certify, without significant steps to break from past self-monitoring requirements, is unlikely to meaningfully improve contractors' cyber hygiene.[22] Fortunately, the DoD can supplement the CMMC 2.0 rollout to assure the program overcomes challenges that have stalled past efforts to compel contractors to monitor their own cybersecurity.

First, the DoD should adopt contractual language that clarifies its authority to evaluate contractor cybersecurity systems throughout contract administration.[23] The DoD should also adopt a related clarification of its remedies when a contractor fails to comply with cybersecurity

---

[15] *See* Assessing Contractor Implementation of Cybersecurity Requirements, 85 Fed. Reg. 61505, 61516 (proposed Sept. 29, 2020) (to be codified at 48 C.F.R. § 204) (describing feedback received in response to draft versions of the CMMC model).

[16] *See* Abigail Stokes & Marcus Childress, *The Cybersecurity Maturity Model Certification Explained: What Defense Contractors Need to Know*, CSO, (Apr. 8, 2020, 3:00 AM), https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html (detailing the release of CMMC version 1.0 on 31 January 2020).

[17] Assessing Contractor Implementation of Cybersecurity Requirements, 85 Fed. Reg. 61505 (proposed Sept. 29, 2020) (to be codified at 48 C.F.R. § 204).

[18] *Strategic Direction for Cybersecurity Maturity Model Certification (CMMC) Program* U.S. DEP'T OF DEF. (Nov. 4, 2021), https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program [hereinafter *CMMC Strategic Direction*].

[19] *See* Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. 64100 (Nov. 17, 2021) (providing an overview of certification requirements under CMMC 2.0).

[20] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at i-ii (describing contractors' failures to "consistently implement DoD-mandated system security controls").

[21] *See infra* Part II.A.

[22] *See infra* Part III.

[23] *See infra* Part IV.A.

requirements.[24] This will allow the DoD to discover and act when contractors have failed to properly certify their cyber compliance, while simultaneously acting as a new source of motivation for contractors to comply and accurately evaluate their own systems.[25] To ensure these efforts have a worthwhile impact, however, the DoD will need to utilize existing resources to give component contracting offices the necessary expertise to conduct meaningful inspections.[26] Finally, the DoD should begin to record the data it has gathered on contractor cybersecurity compliance in a consequential manner.[27] These steps, if executed carefully, will greatly increase the chances that this program succeeds where past efforts have failed, and can help ensure an industrial base prepared to counter our adversaries' attempts to obtain sensitive unclassified information.

Part II of this article provides an overview of the history of contractor cyber networks and systems, the circumstances leading up to the CMMC, and the current state of the CMMC framework. Part III then discusses the risks associated with the current path forward, particularly those associated with relying on contractors to self-certify their cybersecurity systems. Finally, Part IV offers a path to address those risks and recommends implementing guidance.

II. Background

A. Vulnerabilities in Contractor Networks and Systems

While security concerns over information in the hands of contractors have been longstanding,[28] over the last decade those concerns have increasingly focused on the cybersecurity precautions contractors have, or have not, taken.[29] A large catalyst behind this shift has been a series of high-profile breaches of contractor systems by adversaries.[30] High-profile

---

[24] *See infra* Part IV.B.
[25] *See infra* Part IV.
[26] *See infra* Part IV.C.
[27] *See infra* Part IV.D.
[28] *See, e.g.*, U.S. GOV'T ACCOUNTABILITY OFF., GAO-03-1037T, INFORMATION SECURITY: FURTHER EFFORTS NEEDED TO FULLY IMPLEMENT STATUTORY REQUIREMENTS IN DOD 29 (2003) (identifying the security of contractor-provided services as a major point of concern).
[29] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (identifying widespread cybersecurity deficiencies by contractors).
[30] *See Contractors are Giving Away America's Military Edge*, *supra* note 8 (noting the influence of high-profile breaches in describing the need for change).

breaches have included not only the theft of "sensitive data related to naval warfare from the computers of a Navy contractor,"[31] as discussed above, but also the theft of "travel records compromising the personal information and credit card data of U.S. military and civilian personnel"[32] and the theft of F-35 design data,[33] among others.

While these events illustrate individual failures, both internal DoD reviews and Government Accountability Office (GAO) reports have revealed widespread, systemic cybersecurity failures by contractors. The GAO has warned that contractor cybersecurity systems have exposed controlled DoD information, noting in a 2014 report that multiple major agencies, including the DoD, had "reliability issues" just determining which systems were contractor operated.[34] In exploring why these issues were so widespread, the GAO reached the conclusion that "[i]n the past, consideration of cybersecurity . . . was not a focus of key acquisition and requirements policies nor was it a focus of key documents that inform decision-making,"[35] before further noting these failures put weapons systems at risk.[36] Most recently, the GAO indicated that contracting for cybersecurity requirements remains a challenge: "guidance usually did not specifically address how acquisition programs should include cybersecurity requirements . . . and verification processes in contracts."[37]

As early as 2011, the DoD Inspector General found that these issues resulted in serious failures in information security practices by contractors, issuing a report titled "DoD Cannot Ensure Contractors Protected

---

[31] Helene Cooper, *Chinese Hackers Steal Naval Warfare Information*, N.Y. TIMES, (Jun. 8, 2018), https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html.

[32] Lolita C. Baldor, *Pentagon Reveals Cyber Breach of Travel Records*, ASSOCIATED PRESS (Oct. 12, 2018), https://apnews.com/article/7f6f4db35b0041bdbc5467848225e67d.

[33] David Alexander, *Theft of F-35 Design Data is Helping U.S. Adversaries – Pentagon*, REUTERS (June 19, 2013, 2:36 PM), https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619.

[34] U.S. GOV'T ACCOUNTABILITY OFF., GAO-14-612, INFORMATION SECURITY: AGENCIES NEED TO IMPROVE OVERSIGHT OF CONTRACTOR CONTROLS 22-23 (2014).

[35] U.S. GOV'T ACCOUNTABILITY OFF., GAO-19-128, WEAPON SYSTEMS CYBERSECURITY: DOD JUST BEGINNING TO GRAPPLE WITH SCALE OF VULNERABILITIES 17 (2018) [hereinafter GAO ROI-VULNERABILITIES].

[36] *See id.* at 18 (noting that a lack of focus on cybersecurity puts systems and their related missions at risk).

[37] U.S. GOV'T ACCOUNTABILITY OFF., GAO-21-288, HIGH-RISK SERIES: FEDERAL GOVERNMENT NEEDS TO URGENTLY PURSUE CRITICAL ACTIONS TO ADDRESS MAJOR CYBERSECURITY CHALLENGES 53 (2021).

Controlled Unclassified Information for Weapon Systems Contracts."[38] While the cybersecurity of contractor systems has been the subject of DoD Inspector General reports since then,[39] by late 2016, contractor systems were listed as one of the most frequently reported cybersecurity weaknesses challenging the DoD.[40] A 2019 report titled "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems" found that every single contractor evaluated in the DoD Inspector General's sample group had significant failures in establishing basic cybersecurity controls.[41] A 2020 report confirmed that risks related to "contractors and third-party partners" remained ongoing, without significant progress, due to failures to implement necessary cybersecurity measures or controls.[42] These cybersecurity shortcomings pose risks to both national security and personal data that need to be addressed hastily.

B. Unsuccessful Legislative and Regulatory Efforts to Address Challenges

Unfortunately, while these challenges have received significant attention, legislative and regulatory efforts to address them have fallen short. Despite substantial requirements to clean up contractor cybersecurity systems, the DoD's consistent failure to provide means of

---

[38] INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2011-115, DOD CANNOT ENSURE CONTRACTORS PROTECTED CONTROLLED UNCLASSIFIED INFORMATION FOR WEAPON SYSTEMS CONTRACTS (30 Sept. 2011).

[39] *See, e.g.*, INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2015-180, DOD CYBERSECURITY WEAKNESSES AS REPORTED IN AUDIT REPORTS ISSUED FROM AUGUST 1, 2014, THROUGH JULY 31, 2015, at 6-7 (Sept. 25, 2015) (identifying the U.S. Army's continued reliance on voluntary cyber reporting by contractors despite a required DFARS clause language necessitating mandatory reporting as a point of failure).

[40] INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2017-034, DOD CYBERSECURITY WEAKNESSES AS REPORTED IN AUDIT REPORTS ISSUED FROM AUGUST 1, 2015, THROUGH JULY 31, 2016, at 5 (14 Dec. 2016). The report was blunt, specifically stating, "[W]e found that the cyber weaknesses most frequently cited . . . [include] contractor systems . . . ." *Id.*

[41] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (summarizing the flaws identified in each contractor's cybersecurity practices).

[42] *See* INSPECTOR GEN., U.S. DEP'T OF DEF., NO. DODIG-2020-089, SUMMARY OF REPORTS AND TESTIMONIES REGARDING DEPARTMENT OF DEFENSE CYBERSECURITY FROM JULY 1, 2018, THROUGH JUNE 30, 2019, at 12 (11 June 2020) [hereinafter DOD IG REPORTS SUMMARY] (concluding that "significant cybersecurity risks identified in the 46 reports issued and 3 testimonies provided to Congress relate to vendor risk management [and others] . . . . Without adequate controls in those areas, the DoD cannot ensure that . . . contractors and third-party partners implement necessary cybersecurity measures or controls . . . . ").

verification or enforcement have plagued its efforts to improve compliance.

Prior to the CMMC framework, efforts to ensure contractors safeguarded their information systems primarily relied upon mandated breach reporting, threat information sharing, and contractual terms.[43] The first two of these, mandated breach reporting and information sharing, have been helpful but, by their nature, could not ensure satisfactory cyber hygiene. Breach reporting requirements, mandated through the 2013, 2015, and 2019 National Defense Authorization Acts,[44] were not meant to ensure contractors maintained any specific cybersecurity measures. Instead, they were created to ensure awareness of "successful cyber intrusions . . . into the computer networks of operationally critical contractors so that . . . potentially affected combatant commands can assess the risks to contingency operations posed by those intrusions and adjust operational plans, if necessary."[45] Similarly, the DoD's most prominent threat-sharing program for contractors, the Defense Industrial Base Cybersecurity Program, does not require contractors to enact cybersecurity measures or enforce standards.[46] Rather, the voluntary program is simply designed to share information for use in countering threats without prescribing a method or course of action to do so.[47]

Contract terms, on the other hand, have required contractors to meet specific cybersecurity precautions, but have had mixed success. Since 2013, the DoD has used mandatory clauses in the DFARS to require

---

[43] Although these three tools made up the bulk of existing legislative and regulatory mechanisms for encouraging contractor cybersecurity pre-CMMC, it should be noted that these have existed for a relatively short period of time themselves. For a deeper history of cybersecurity requirements as they applied to acquisitions prior to the introduction of these tools see Kui Zeng, Exploring Cybersecurity Requirements in the Defense Acquisition Process (Apr. 23, 2016) (D.Sc. dissertation, Capitol Technology University), (ProQuest).

[44] *See* 10 U.S.C. § 393 (requiring "[r]eporting on penetrations of networks and information systems of certain contractors," and originally enacted by Section 941 of the National Defense Authorization Act for 2013, Pub. L. No. 112-239, 126 Stat. 1632 (2013); *see also* 10 U.S.C. § 391 (requiring "[r]eporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors," and originally enacted by section 1632 of the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113-291, 128 Stat. 3292 (2014)); 10 U.S.C. § 2224 note (instituting "[r]eporting [r]equirements for [c]ross [d]omain [i]ncidents and [e]xemptions to [p]olicies for [i]nformation [t]echnology," and originally enacted by section 1639 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636 (2018)).

[45] S. REP. NO. 113-176, at 229 (2014).

[46] *See* 32 C.F.R. § 236.1 (2023) (describing the purpose of the Defense Industrial Base Cybersecurity program).

[47] *See* 32 C.F.R. § 236.6 (2023) (detailing the general provisions of the DoD's Defense Industrial Base Cybersecurity program).

contractors and subcontractors to "provide adequate security on all covered contractor information systems."[48] "Adequate security" is defined as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."[49] More specifically, the DFARS mandates that "the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.'"[50] Since 2016, the Federal Acquisition Regulation (FAR) section 52.204-21 has also imposed additional obligations on non-DoD contractors with the intent to improve cybersecurity practices, which complement the DFARS clauses and NIST SP 800-171.[51] The DFARS clause incorporating NIST SP 800-171 is generally required on all contracts (with limited exceptions),[52] while the clause at FAR 52.204-21 is required on contracts where the contractor or any subcontractor "may have Federal contract information residing in or transiting through its information system" (again with limited exceptions).[53] Both the FAR and DFARS requirements must be passed on to subcontractors by the contractor if the covered sensitive unclassified information will be handled by the subcontractor.[54]

Taken together, these requirements were meant to provide sufficient, if minimum, cybersecurity requirements for contractors to meet their contractual obligations and keep sensitive unclassified information secure. These resources contain the most direct guidance available to contractors in establishing adequate systems. The NIST SP 800-171 provides a series

---

[48] DFARS 204.7302(a)(1) (2022).
[49] DFARS 204.7301 (2022).
[50] DFARS 252.204-7012 (2022).
[51] *See* FAR 52.204-21 (2022) (establishing fifteen minimum requirements for the safeguarding of covered contractor information systems). The language of this clause is required generally by FAR 4.1903 (2022), and in solicitations and contracts for the acquisition of commercial products or commercial services, other than commercially available off-the-shelf items by FAR 12.301(d)(5) (2022).
[52] *See* DFARS 204.7304 (2022) (establishing guidelines for the inclusion of covered defense information clauses).
[53] *See* FAR 4.1903 (2022) (establishing when the insertion of the clause at 48 C.F.R. § 52.204-21 is required).
[54] *See* FAR 52.204-21(c) (2022) ("The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts . . . in which the subcontractor may have Federal contract information residing in or transiting through its information system."). *See also* DFARS 252.204-7012(m) (2022) ("The Contractor shall . . . [i]nclude this clause . . . in subcontracts . . . for operationally critical support, or for which subcontract performance will involve covered defense information . . . . The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause . . . .").

of obligations, all of which fall within fourteen "families" of cybersecurity requirements: (1) access control; (2) awareness and training; (3) audit and accountability; (4) configuration management; (5) identification and authentication; (6) incident response; (7) maintenance; (8) media protection; (9) personnel security; (10) physical protection; (11) risk assessment; (12) security assessment; (13) system and communications protection; and (14) system and information integrity.[55] Similarly, FAR 52.204-21 provides fifteen minimum requirements which, for the most part, mirror requirements contained within the NIST SP 800-171 families.[56]

Despite the premise that these requirements should result in sufficiently protected contractor cybersecurity systems, contractor cybersecurity practices have continued to fall short of expectations. Internal reviews and a number of high-profile incidents since the implementation of both the DFARS and FAR requirements make that clear.[57] While there are likely a multitude of reasons for each specific failure, the systemic issues have largely been attributed to the lack of effective verification and enforcement of their terms.[58]

Verification and enforcement have remained a challenge for several reasons. Perhaps most importantly, "neither the FAR clause, nor the DFARS clause, provide for DoD verification of a contractor's implementation of basic safeguarding requirements or the security requirements specified in NIST SP 800-171."[59] The lack of a broad verification program left it up to contracting offices to ensure compliance

---

[55] RON ROSS ET AL., NAT'L INST. OF STANDARDS AND TECH., SP 800-171 REV. 2: PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS 9-40 (2021).

[56] *See* FAR 52.204-21(b) (2022). *Compare, e.g.*, FAR 52.204-21(b)(1)(iii) (2021) (requiring contractors to "[v]erify and control/limit connections to and use of external information systems") *with* NAT'L INST. OF STANDARDS & TECH., *supra* note 55, para. 3.1.2 (requiring contractors to "[v]erify and control/limit connections to and use of external systems").

[57] *See, e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at i-ii (finding that all the contractors audited in the sample group evaluated "did not consistently implement DoD-mandated system security controls for safeguarding Defense information"). *See also Contractors are Giving Away America's Military Edge*, *supra* note 8 (detailing numerous high-profile breaches of contractor systems that occurred after the introduction of NIST SP 800-171 requirements).

[58] *See* U.S. DEP'T OF DEF., DFARS CASE 2019-D041: ASSESSING CONTRACTOR IMPLEMENTATION OF CYBERSECURITY REQUIREMENTS REGULATORY IMPACT ANALYSIS 4 (2020) [hereinafter CYBERSECURITY REQUIREMENTS RIA] (discussing the impact of a lack of verification mechanisms in the cybersecurity contract clauses of the FAR and DFARS).

[59] *Id.*

in awarding and administering contracts,[60] despite the fact that those contracting offices entrusted with monitoring or verification often had no background in the subject.[61] Even when cybersecurity issues were brought to a contracting office's attention, many were still unable to verify compliance or enforce standards because they either felt incapable of acting without higher-headquarters or DoD guidance,[62] did not feel they had "the resources to review compliance,"[63] or did not feel they had the contractual authority to audit contractor systems.[64] As a result, "contracting offices and requiring activities did not implement processes to verify that contractors complied with Federal and DoD requirements for protecting [controlled unclassified information] maintained in non-Federal systems and organizations."[65] This was compounded by the fact that contracting offices did not prioritize cybersecurity and the protection of sensitive unclassified information when evaluating whether to award a contract (or when monitoring a contract during its administration) if they were not the primary focus of a contract's subject matter.[66] Without

---

[60] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 5-6 (reviewing the responsibility of contracting offices to establish procedures for verifying compliance with cybersecurity contractual requirements, and the failure of those offices to do so). The Defense Counterintelligence and Security Agency (DCSA), by the 17 May 2018 designation of the Office of the Under Secretary of Defense for Intelligence, was tapped to take over many of these responsibilities "as the lead agency for providing oversight of Controlled Unclassified Information (CUI) maintained by DoD contractors." *Id.* at 3. Those responsibilities were enhanced by the publication of DoD Instruction 5200.48, which provided further guidance concerning CUI. U.S. DEP'T OF DEF., INSTR. 5200.48, CONTROLLED UNCLASSIFIED INFORMATION (CUI) (2020). However, DCSA indicates that it is "not currently conducting any oversight of CUI associated with . . . cleared contractors at this time." *Controlled Unclassified Information*, U.S. DEF. COUNTERINTEL. & SEC. AGENCY, https://www.dcsa.mil/mc/ctp/cui (last visited Feb. 7, 2023).

[61] *See*, *e.g.*, DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (detailing how a contracting officer representative tasked with monitoring a contract was unaware of the relevant clauses and path towards NIST SP 800-171 compliance).

[62] *See*, *e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (describing how "[a] Defense Contract Management Agency official . . . stated that the agency was waiting for DoD guidance to establish an assessment process to verify contractor compliance" as the reason the agency had not conducted oversight activities).

[63] DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28.

[64] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (summarizing how multiple agencies reported their position did not have contractual authority to audit contractor systems to ensure compliance with contractual requirements and NIST SP 800-171).

[65] DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 4.

[66] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 32 (revealing that DoD contracting offices often "did not always know which contracts required contractors to maintain [controlled unclassified information] . . . . [and] the DoD does not have a

verification and enforcement, contractors' protection of sensitive unclassified information has not improved.[67]

C. Introduction of the CMMC Framework

As a result of these persistent challenges, the DoD overhauled its approach to contractor cybersecurity by introducing the CMMC framework, which expanded cybersecurity requirements and sought to tackle verification shortcomings.

The initial version of CMMC built upon NIST SP 800-171 and modified the applicable cybersecurity requirements for contractors.[68] The initial framework included tiered standards of cybersecurity, with five CMMC certification levels based on the information the contractor would handle under the contract.[69] While level one certifications essentially required the same security measures as FAR section 52.204-21, security standards increased at each tier under the framework.[70] For example, certification level three, which was standard for contracts handling any controlled unclassified information (CUI), required all of the security levels prescribed in NIST SP 800-171 through DFARS clause 252.204-7012, along with twenty additional practices and three processes.[71]

Beyond this reorganization of security requirements, the original CMMC framework's most novel advancement was the introduction of a verification process for contractors' security practices. It required that, prior to contract award, all contractors pass an assessment at the appropriate CMMC level within the last three years and maintain a current (completed within the last three years) CMMC certification for the duration of the contract.[72] "Third Party Assessment Organizations," or "C3PAOs," conducted the assessments, not the DoD.[73] The process was

process in place to track which contractors maintain [controlled unclassified information]"). *See also* GAO ROI-VULNERABILITIES, *supra* note 35, at 17 (reporting "consideration of cybersecurity was not a focus of the key processes" relating to the acquisition of weapon systems).

[67] *See* DOD IG REPORTS SUMMARY, *supra* note 42, at 12 (noting the continuing failure to make progress in ensuring contractors implement necessary cybersecurity measures).

[68] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12 (describing the CMMC framework).

[69] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12.

[70] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12-13.

[71] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 13.

[72] DFARS 252.204-7021(b) (2022).

[73] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12 (describing the CMMC contractor assessment process).

market-based; the contractor seeking certification would pay the assessment costs,[74] while C3PAO would pay their own the accreditation costs.[75]

Importantly, these verification requirements would have "flowed down to subcontractors at all tiers," with prime contractors no longer at liberty to distinguish which subcontractors were required to meet cybersecurity standards.[76] Section 252.204-7021 of DFARS was set to begin applying this original CMMC framework to select contracts in fiscal year 2021,[77] with a slow buildup before applying "to all business entities that are awarded a DoD contract" after 1 October 2025.[78]

While this framework seemed poised to aggressively combat the verification and enforcement issues that plagued the contract-based cybersecurity requirements, the program, for a variety of reasons, encountered significant headwinds.[79] In particular, the need to pay for certification was expected to pose substantial costs on small businesses,[80] potentially limiting the DoD's market.[81] There were also very real

---

[74] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 15 (indicating that the "cost of these CMMC assessments will be driven by multiple factors including market forces, the size and complexity of the network or enclaves under assessment, and the CMMC level"). There was initially some indication that these costs would be considered an "allowable cost," which could be reimbursed by the DoD. *See*, *e.g.*, *CMMC Preparation Is An "Allowable Cost" And Reimbursable by DoD*, SYSARC (Aug. 6, 2019), https://www.sysarc.com/cyber-security/cmmc-preparation-is-an-allowable-cost-and-reimbursable-by-dod. However, there is considerable debate that this would be possible, and the DoD has recently removed all previous references to reimbursement from its CMMC material. *See CMMC FAQs*, CHIEF INFO. OFFICER: U.S. DEP'T OF DEF., https://dodcio.defense.gov/CMMC/FAQ/#AboutCMMC (last visited Feb. 7, 2023).

[75] *See* Sara Friedman*, CMMC Accreditation Body Clarifies Details of Approval Process for Assessment Organizations*, INSIDE DEF., (Sept. 2, 2021), https://www.insidedefense.com/share/212555 (stating the requirements for C3PAO assessor certification).

[76] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 16.

[77] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 12. *See also* Letter from Info. Tech. Indus. Council, et al., to Honorable Kathleen Hicks, Deputy Sec'y of Def. (Sept. 8, 2021), https://www.itic.org/documents/public-sector/MultiassociationLetter_CybersecurityPolicy_September2021.pdf.

[78] CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 16.

[79] *See CMMC FAQs*, *supra* note 74 (discussing why the DoD transitioned from CMMC 1.0 to CMMC 2.0).

[80] *See* Jackson Barnett, *Department of Defense to Address Small Business Concerns as Part of CMMC Program Review*, FEDSCOOP (June 28, 2021), https://www.fedscoop.com/department-of-defense-to-address-small-business-concerns-as-part-of-cmmc-program-review (detailing concerns with the cost of CMMC certification for small businesses).

[81] *See, e.g.*, *CMMC Implementation: What It Means for Small Businesses: Hearing Before the H. Small Bus. Subcomm. on Oversight, Investigations & Regul. of the H. Small Bus. Comm.,* 117th Cong. (2021) (statement of Michael Dunbar, President, Ryzhka International).

concerns that the plan to independently certify the approximately 300,000 DoD contractors was simply not feasible.[82] These concerns increased when the number of assessors fell far short of initial estimates.[83]

In response to these issues, the DoD drastically changed its CMMC implementation plan in November of 2021 when it released initial plans for "CMMC 2.0."[84] While specifics regarding the new framework remain in development, some changes are clear. First, the standards more closely align with NIST standards, eliminating maturity processes and security practices unique to the CMMC.[85] Second, the DoD removed levels two and four from the five CMMC certification levels, which were transitional and allowed contractors to smoothly move between levels one, three, and five.[86] Under the new system, contractors who handle "Federal Contract Information"[87] (FCI) will require a level-one certification, those who handle any CUI[88] will require a level-two certification, and those contractors facing a particularized risk from "Advanced Persistent Threats" will be required to obtain a level-three certification.[89] Most importantly for our purposes, the third-party assessment framework was

---

[82] *See,* Federal Drive with Tom Temin, *DoD's Plan for Contractor Cybersecurity Lacks a Few Things, Money's Only One of Them*, FED. NEWS NETWORK (June 18, 2021, 12:55 PM), https://federalnewsnetwork.com/cybersecurity/2021/06/dods-plan-for-contractor-cybersecurity-lacks-a-few-things-moneys-only-one-of-them.

[83] *Id.*

[84] *See CMMC Strategic Direction*, *supra* note 18 (announcing the launch of CMMC 2.0 and describing changes from CMMC 1.0 in broad terms).

[85] Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. 64100 (Nov. 17, 2021).

[86] *Id.*

[87] "Federal Contract Information" is defined within the CMMC framework as "information provided by or generated for the Government under contract not intended for public release." CARNEGIE MELLON UNIV. & THE JOHNS HOPKINS UNIV. APPLIED PHYSICS LAB'Y, Cybersecurity Maturity Model Certification (CMMC) Model Overview 1 (2021), https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview_V2.0_FINAL2_20211202_508.pdf (citing 48 C.F.R. § 252.204-21 (2016)).

[88] "Controlled Unclassified Information" is defined within the CMMC framework as "information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended." CARNEGIE MELLON UNIV. & THE JOHNS HOPKINS UNIV. APPLIED PHYSICS LAB'Y, *supra* note 87, at 1 (citing NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COM., SP 800-171, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS 9-40 (2nd rev. 2021)).

[89] *See* CARNEGIE MELLON UNIV. & THE JOHNS HOPKINS UNIV. APPLIED PHYSICS LAB'Y, *supra* note 87, at 16 (summarizing the criteria for each level of certification under the CMMC).

removed for both level-one contractors,[90] who constitute the vast majority of DoD contractors,[91] and those level-two contractors involved with "non-prioritized acquisitions," which is estimated to be approximately half of the contractors handling CUI.[92] The third-party assessment for both of these groups has instead been replaced by an annual self-assessment.[93]

The return to a self-assessment framework once again puts the majority of contractors in a position to self-certify compliance with relevant cybersecurity requirements. While the pivot to CMMC 2.0 provided necessary relief to what would have been a significantly overburdened assessment system and a scrambling industrial base, self-assessments bring back the same set of challenges the DoD wrestled with in its past efforts to ensure effective cybersecurity. Third-party assessors brought accountability[94] to a population that often failed to uphold its cybersecurity responsibilities when allowed to self-monitor.[95] The return to contractor-led compliance, on the other hand, maintains the status quo despite its lack of success.

---

[90] Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. 64100 (Nov. 17, 2021) (providing an overview of certification requirements under CMMC 2.0).

[91] *See* Jason Doubleday, *Pentagon Strips Down CMMC Program to Streamline Industry Cyber Assessments*, FED. NEWS NETWORK (Nov. 4, 2021, 2:09 PM), https://www.federalnewsnetwork.com/defense-main/2021/11/pentagon-strips-down-cmmc-program-to-streamline-industry-cyber-assessments.

[92] *See* Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. at 64100. There has been some indication that this may change in the future, and all level-two contractors will be required to obtain a third-party CMMC assessment. *See* Jason Doubleday, *More Companies May Have to Get a CMMC Assessment After All*, FED. NEWS NETWORK (Feb. 10, 2022, 6:42 PM), https://www.federalnewsnetwork.com/cybersecurity/2022/02/more-companies-may-have-to-get-a-cmmc-assessment-after-all. However, the official position of the DoD remains that only a portion of companies handling CUI will be required to obtain a third-party assessment. *See CMMC FAQs*, *supra* note 74 (indicating that only "some" level-two contractors will be required to obtain a third-party assessment).

[93] *See* Cybersecurity Maturity Model Certification (CMMC) 2.0 Updates and Way Forward, 86 Fed. Reg. at 64100 (providing an overview of requirements under CMMC 2.0).

[94] *See* Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), 85 Fed. Reg. 61505 (proposed Sept. 29, 2020) (to be codified at 48 C.F.R. § 204) (outlining third party accessor requirements of CMMC 1.0).

[95] *See* discussion *supra* Part II.B (summarizing contractor cybersecurity challenges).

III. Challenges to Effective Certification Under the New Self-Evaluation Framework

The ongoing reliance on self-evaluations, without outside review, is a real issue that impacts national security; weak systems that provide an avenue for adversaries to access FCI and CUI have repeatedly enabled them to counter our abilities and expand their own.[96] The status quo must change. Self-evaluation as a primary means of accountability for DoD contractors is a tried and failed approach.[97] Mandatory FAR and DFARS provisions have required DoD contractors to meet cybersecurity standards for years.[98] Contractors, however, were left to self-monitor their compliance under that framework, and the result has been an almost uniform failure to effectively do so.[99] The recent withdrawal of third-party certification requirements without any substantial substitution to motivate contractor compliance essentially brings requirements full circle.[100] The plan lacks any truly novel means of review or enforcement not present under the previous framework.

Removing third-party assessments also removes a significant source of expertise without an obvious replacement. Many contracting offices lack the expertise to internally verify compliance even if they identify an issue.[101] The third-party assessor program addressed this challenge by providing a host of resources and an assessor who could evaluate efforts, identify weaknesses, and knowledgeably evaluate compliance.[102] With

---

[96] *See, e.g.*, Ellen Nakashima & Paul Sonne, *supra* note 1 (describing the impact of the loss of sensitive, unclassified FCI and CUI to the Chinese Ministry of State Security).

[97] *See* discussion *supra* Part II.B (describing the failures of the contractual clause requirements in establishing effective contractor cyber hygiene).

[98] *See* DFARS 204.73 (2022) (detailing cybersecurity requirements for FCI and CUI). *See also* FAR 52.204-21 (2022) (establishing 15 minimum requirements for the safeguarding of covered contractor information systems).

[99] *See* DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at i-ii (finding that all the contractors audited in the sample group evaluated "did not consistently implement DoD-mandated system security controls for safeguarding Defense information"). *See also Contractors are Giving Away America's Military Edge*, *supra* note 8 (detailing numerous high-profile breaches of contractor systems that occurred after the introduction of NIST SP 800-171 requirements).

[100] Self-assessments will be conducted along the same standards that existed prior to CMMC implementation. The only additional requirement is "an annual affirmation by a senior company official." *CMMC Assessments*, CHIEF INFO. OFFICER, U.S. DEP'T OF DEF., https://dodcio.defense.gov/CMMC/Assessments (last visited Feb. 7, 2023) (previewing the assessment process under CMMC 2.0).

[101] *See* DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (describing contracting office's lack of understanding of cybersecurity systems and requirements).

[102] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 13-15 (describing the role of assessors in the CMMC framework).

that program gone, contracting offices are left in some cases to do little more than guess whether contractors have appropriately addressed requirements.

These challenges are significant. Cumulatively, the return to a self-evaluation model, the absence of any new means of enforcement, and the lack of cybersecurity knowledge amongst contracting offices threaten to prevent the CMMC framework from reaching its most important goal: ensuring contractors meet appropriate cybersecurity requirements.[103] The question then becomes: what actions can be taken to address these challenges within the CMMC 2.0 framework in order to ensure that goal is met?

IV. Necessary Steps to Ensure Effective Self-Evaluations

Now, as the DoD is finalizing and preparing rules for CMMC 2.0, is the moment to take action to address the challenges associated with self-evaluations. This can be done by allowing a robust inspection system to flourish. To do so, the DoD should first clarify rights of access to allow contracting offices to effectively monitor contractors' self-evaluations. This can be done by updating mandatory clauses in the DFARS, or, in the interim, through the inclusion of contract-specific clauses.[104] Second, contracting officers' remedies to correct and deter deficiencies must be clarified.[105] Third, contracting offices need to effectively utilize clarified rights of access, and remedies, to effectively audit contractors, identify failures, and motivate others to self-evaluate. As discussed below, using locally appointed government technical monitors can achieve these goals without expending vast resources.[106] Finally, the DoD can, and should, ensure it retains the data from this inspection framework to document contractor past performance and identify systemic difficulties in cybersecurity compliance so that it can better address future challenges.[107]

---

[103] *See About CMMC*, CHIEF INFO. OFFICER, U.S. DEP'T OF DEF., https://www.dodcio.defense.gov/CMMC/About (last visited Feb. 7, 2023) (describing the CMMC program).
[104] *See infra* Part IV.A.
[105] *See infra* Part IV.B.
[106] *See infra* Part IV.C.
[107] *See infra* Part IV.D.

A. Clarifying Contractual Cybersecurity Monitoring Authorities

Without a means of verifying contractor cyber hygiene prior to contract formation, attempts to ensure cybersecurity requirements are fulfilled must shift to the contract management phase. Yet, as discussed above,[108] multiple DoD agencies believe they are essentially powerless during this period, stating that they do "not have the contractual authority to oversee compliance on contractor networks."[109] That must change if any effective means of verification and enforcement are to take place, and it is imperative that clear contractual authority to inspect contractor cybersecurity systems be a part of the modified CMMC framework going forward.

"Inspection . . . is the primary means of ensuring that the government receives that for which it bargained."[110] The FAR, recognizing this importance, requires agencies to "ensure that . . . contracts include inspection . . . requirements . . . [and that] [n]o contract precludes the Government from performing inspection."[111] Similarly, the DFARS recognizes the importance of inspection in ensuring contract requirements are met, requiring "[d]epartments and agencies . . . [to] [a]pply Government quality assurance to all contracts for services and products . . . [and] [c]onduct quality audits to ensure the quality of products and services meet contractual requirements."[112]

All of these requirements emphasize one thing: if a good or service is an important part of contract performance, the contract should provide the Government with a means of inspection.[113] The CMMC framework is, at its core, a push to make adherence to contractual cybersecurity

---

[108] *See supra* Part II.B.

[109] DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28. There appears to be some debate about whether contractual authority to oversee compliance exists among DoD agencies. *See id.* (discussing the confusion around whether assessing contractor networks and systems is permissible). Inspections that occur but were unforseen by contract can have several negative consequences for the government, including the obligation to cover increased costs to the contractor. *See* JOHN CIBINIC, JR. ET AL., ADMINISTRATION OF GOVERNMENT CONTRACTS 700-06 (5th ed. 2016) (describing the impact of improper inspections). Even if access to contractor networks were eventually found to be permissible under current default contract language by a reviewing authority, the existing confusion even among DoD components means that the current default language presents at the very least the risk of litigation and associated delays.

[110] CIBINIC, JR. ET AL., *supra* note 109, at 698.

[111] FAR 46.102(d) (2022).

[112] DFARS 246.102(1)-(2) (2022).

[113] *See, e.g.*, DFARS 246.102 (2022) (detailing DoD's systemic quality assurance program to ensure contract performance to specified requirements).

requirements a critical component of contract performance.[114] The first step toward aligning these goals is a right of access in all contracts involving sensitive unclassified information so that cyber hygiene can be inspected and evaluated just like other critical components of contract performance.

This can be accomplished in two ways. First, and most immediately, DoD contracting offices can individually insert clear, unambiguous clauses into future contracts that ensure a right to inspect information systems. Right to inspect clauses "would allow representatives of the agencies to assess the cybersecurity protections implemented on contractor networks and systems,"[115] as the DoD Inspector General has advocated regarding contractors maintaining CUI.[116] These clauses could be modeled upon existing language that allows for inspection rights,[117] and would overcome DoD agencies' concern that they do "not have the contractual authority to oversee compliance on contractor networks."[118] With a clear method to evaluate cybersecurity self-assessments enshrined in the contract, contractors are also put on notice that inspections of their cybersecurity systems and self-evaluations are a distinct possibility, increasing motivations to improve compliance.

In the long term, however, clauses prepared for individual contracts on an ad-hoc, local basis carry minor risks. These risks range from the relatively harmless, such as failing to ensure a sufficiently broad right of access to systems,[119] to the more serious risk of failing to provide for the proper type of inspection, potentially preventing a meaningful assessment,[120] or even allowing the contractor to recover costs in the

---

[114] *See About CMMC*, *supra* note 103 (describing the renewed priority of cybersecurity in DoD contracting).

[115] DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28-29.

[116] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28-29 (advocating for the adoption of right-to-audit statements in contracts by DoD component contracting offices).

[117] *See, e.g.,* FAR 52.227-14 (2022) (Alternate V) (allowing the contracting officer the opportunity to "inspect at the Contractor's facility any data withheld" to verify the contractor's assertion of limited rights of data or for evaluating work performance). *See also* FAR 52.246-12 (2022) (inspection of construction clause); FAR 52.246-4 (2022) (inspection of services clause).

[118] DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28.

[119] *See* CIBINIC, JR. ET AL., *supra* note 109, at 706-07 (discussing the impact of the language used in inspection clauses on the permissible place and time of ensuing inspections).

[120] *See* CIBINIC, JR. ET AL., *supra* note 109, at 701-05 (analyzing the impact of language used in inspection clauses on the types of inspections the government may perform).

future.[121] Standardized, mandatory inspection clauses, paired with the mandatory cybersecurity requirements in DFARS 252.204-7012[122] and FAR 52.204-21,[123] and any additional requirements implemented by CMMC 2.0 can solve these problems.[124] A thoroughly prepared and vetted mandatory right-to-inspect clause can provide for the necessary inspections to evaluate compliance with minimal risk of an oversight that could cause problems later.[125] With the risk minimized, the mandatory clause can guarantee a right of access and put contractors on notice that their self-certifications will be evaluated, just as individually inserted clauses would seek to do in the short term.

Failing to move forward with clear right of access clauses leaves few other measures for the DoD to verify contractors' cybersecurity assertions. Relying on current contract language is, as discussed above, insufficient to ensure DoD can verify compliance at any stage of the contracting process.[126] The DoD could, alternatively, move towards a framework in which verification is outsourced to third parties or conducted prior to contract formation, as opposed to seeking to clarify its own right of access during contract administration. However, these options were contemplated by CMMC 1.0[127] and eventually rejected.[128] There was insufficient third-party interest to support the large number of assessors necessary to support

---

[121] *See, e.g.*, Appeal of Kenyon Magnetics, Inc., 1977 GSBCA LEXIS 103 (Gen. Serv. Admin. B.C.A., Sept. 30, 1977) (in which the contract failed to put the contractor on notice regarding the inspection conducted, and associated delays allowed an equitable adjustment).

[122] DFARS 252.204-7012 (2022).

[123] FAR 52.204-21 (2022).

[124] *See About CMMC*, *supra* note 103 (indicating that the DoD "intends to pursue rulemaking" at both Part 32 and Part 48 of the Code of Federal Regulations in implementing CMMC 2.0).

[125] There is still the risk that the mandatory clause could be inadvertently left out of the contract, of course, but that risk is minimal. Regular, important emphasis on the significance of such a clause could eliminate this minimal risk if it leads to the clause's inclusion in future contracts under the *Christian* doctrine, first enunciated in G.L. Christian & Assocs. v. United States, 312 F.2d 418, 426 (Ct. Cl. 1963). *See* Michael D. Pangia, *The Unpredictable and Often Misunderstood Christian Doctrine of Government Contracts: Proposed Approaches for Removing Harmful Uncertainty*, 49 Pub. Cont. L.J. 617, 629-35 (2020) (providing an overview of current requirements for reading an absent clause into a government contract under the *Christian* doctrine).

[126] *See* discussion *supra* Part III.

[127] *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 14-15 (laying out a plan in which all contractors handling FCI and CUI were assessed by third-party evaluators prior to contract performance).

[128] *See About CMMC*, *supra* note 103 (stating that all contractors only handling FCI, and a portion of contractors handling CUI, would not undergo third-party assessments or any other sort of outside assessment prior to contract performance).

such a large number of third-party assessments,[129] and the cost was prohibitive.[130] Similarly, shifting evaluations to the contract formation stage would quickly become overwhelming because the DoD would need to consider evaluating not just successful awardees, but also all competing contractors, increasing its workload many times over. Instead, by ensuring a right of access during contract administration, the DoD maintains the ability to evaluate systems and motivate compliance, but on a manageable scale.

B. Establishing Remedies

With a clearer authority to oversee and inspect cybersecurity on contractor networks, the DoD can address concerns that arise during inspections by creating and clarifying contractual noncompliance remedies. Inspections are generally paired with consequences to motivate compliance[131] because the risk that the benefits of the contract may be lost through noncompliance lies at the core of the overall effectiveness of the inspection framework.[132] The DoD does currently have some tools available should it discover concerns, and continued reliance on these tools represents the primary alternative to instituting new contractual language specifying additional remedies. However, there are significant benefits to inserting language in the DFARS that creates and clarifies contracting offices' remedies for noncompliance, and the DoD could easily include such language in the proposed inspection clause discussed above.

A significant body of research on the interrelations between inspections and compliance "reinforce[s] the importance of inspections for compelling compliance."[133] While the mere possibility that an inspection may occur is often enough to motivate compliance,[134] consequences for

---

[129] *See* Christopher Burgess, *Lack of C3PAO Assessors Jeopardizes DoD CMMC Certification Goal*, CSO (Sept. 8, 2021, 2:00 AM), https://www.csoonline.com/article/3632398/lack-of-c3pao-assessors-jeopardizes-dod-cmmc-certification-goal.html (reporting that only 100 approved assessors had obtained certification despite the need for 5,000 to meet requirements under the original CMMC framework).

[130] *See* Barnett, *supra* note 80 (discussing the financial impact of third-party CMMC assessments on small businesses).

[131] *See* Peter J. May, *Compliance Motivations: Affirmative and Negative Bases*, 38 L. & SOC'Y REV. 41, 45 (2004) (discussing the impact of inspection frequency, thoroughness, and consequences on compliance across a range of studies).

[132] *See id.*

[133] *Id.*

[134] *See id.* (comparing the impact of inspections on compliance with the impact of sanctions resulting from those inspections).

noncompliance are an important additional step, capable of ensuring that those who may not otherwise be inclined to comply are convinced to do so.[135] Consequences not only motivate the deficient contractor, but also deter others by making them aware of the potential costs of non-compliance.[136] This is most effective when the potential consequences are clear, known, and predictable.[137]

Unfortunately, the consequences for noncompliance with DoD cyber requirements have been unclear and unenforced, even when deficiencies are well known.[138] The DoD currently has several options to address contractor performance, which it could continue to rely on exclusively for cybersecurity failures. These include, but are not limited to, breach of contract claims,[139] terminations,[140] and causes of action under the False Claims Act (FCA).[141] However, there are concerns with each of these remedies in the cybersecurity context.

Regarding any breach claims, the biggest impediment is that damages will often be impossible to prove absent a known security breach with an accompanying loss of data.[142] Without known damages, a breach of contract claim carries no substantial penalty.[143] Terminations, likewise,

---

[135] *See id.* at 43 (providing an overview of "[t]he traditional toolkit for obtaining compliance . . . through enforcement actions and imposition of sanctions for those found to be out of compliance").

[136] *See id.* at 42 (discussing the deterrent basis for compliance).

[137] *Id.* Importantly, the severity of these consequences is generally not the most significant factor behind their effectiveness. *See id.* at 46 (noting "mixed" outcomes of studies concerning the effect of the level of sanctions on compliance).

[138] *See* DOD IG ROI- CONTRACTOR-OWNED NETWORKS, *supra* note 11, at iii (describing contracting offices' confusion regarding contractor systems and its impact on correcting performance).

[139] Government claims for breach of contract remain available even when the contract does not provide for a specific relief. *See PAE Int'l.*, ASBCA 45314, 98-1 BCA ¶ 29,347 (indicating that "[o]n the other hand, 'when only partial relief is available under the contract . . . the remedies under the contract are not exclusive and the . . . [party seeking damages] may secure damages in breach of contract'" in finding that the Government could recover damages caused by the contractor's theft of fuel) (quoting United States v. Utah Construction and Mining Co., 384 U.S. 394, 402 (1996)).

[140] For default or convenience. *See, e.g.*, FAR 52.249-2 (2022) (termination for convenience of the government clause for fixed-price contracts).

[141] *See* 31 U.S.C. § 3729 (containing the civil provision of the False Claims Act). *See also* 18 U.S.C. § 287 (containing the criminal provisions of the False Claims Act).

[142] *See PAE Int'l.*, ASBCA 45314, 98-1 BCA ¶ 29,347 (indicating that an "injured party in an action for breach of contract is [only] entitled to recover for two types of loss: 'the loss in the value to him of the other party's performance caused by its failure or deficiency' and 'any other loss, including incidental or consequential loss, caused by the breach . . . .'") (quoting the RESTATEMENT (SECOND) OF CONTRACTS § 347 (AM. L. INST. 1981) (Measure of Damages in General)).

[143] *See id.*

are of limited utility. A termination ends contract performance,[144] which may work in some circumstances, but leaves little room to be a useful tool to encourage compliance if the requiring activity does not have the flexibility to overcome the loss of the contract prematurely.

In cases in which the contractor has falsely certified that their system meets cyber requirements, the FCA is perhaps the most on-point remedy, and is currently one of the recommended tools to address lax contractor cybersecurity.[145] Despite this, there are significant concerns to utilizing the FCA as the main tool to address failures. First, it is not a guaranteed solution. FCA liability can only be imposed when the requirement is "material."[146] Whether cybersecurity requirements will meet the definition of material in most contracts is an open dispute, and at least one reviewing authority has determined that such requirements are not material, at least under certain circumstances.[147]

FCA claims must also show that any noncompliance was done "knowingly."[148] This is also a potential point of failure as it will be difficult for the Government to meet its burden.[149] Even if these concerns were satisfied, however, FCA claims are a drastic remedy in which the DoD loses some control and the Department of Justice becomes the lead agency to pursue serious civil or even criminal consequences.[150]

This is simply not a feasible solution for improving compliance when, under the most recent internal DoD audits, essentially *every contractor* is

---

[144] *See, e.g.*, FAR 52.249-2 (2022).

[145] *See Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, U.S. DEP'T OF JUST. (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative (stating that "[t]he Civil Cyber-Fraud Initiative will utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients").

[146] "Material" is defined as "having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property." 31 U.S.C. § 3729(b)(4).

[147] *See* United States *ex rel.* Adams v. Dell Computer Corp., 496 F. Supp. 3d 91 (D.D.C. 2020) (dismissing the *qui tam* suit on the basis that noncompliance with cybersecurity requirements was not material).

[148] "Knowingly" requires that the contractor "(i) has actual knowledge of the information; (ii) acts in deliberate ignorance of the truth or falsity of the information; or (iii) acts in reckless disregard of the truth or falsity of the information." 31 U.S.C. § 3729(b)(1).

[149] *See, e.g.*, Michael Wagner et al., *Cybersecurity and Government Contracting: False Claims Act Considerations*, COVINGTON, (Jan. 11, 2021), https://www.insidegovernment contracts.com/2021/01/cybersecurity-and-government-contracting-false-claims-act-considerations (detailing concerns regarding the requirement to show noncompliance was "knowing" in the context of cybersecurity FCA claims).

[150] *See* 31 U.S.C. § 3729 (containing the civil provision of the False Claims Act). *See also* 18 U.S.C. § 287 (containing the criminal provisions of the False Claims Act).

failing to meet some of their low-level cybersecurity requirements.[151] The DoD does not, and would not, use the FCA in other contexts to address every instance of contractor underperformance, and it should not with cybersecurity. To do so would be inappropriately heavy-handed; relying on sanctions of this nature to address such common issues will likely degrade trust and legitimacy and will harm compliance efforts more than help them.[152]

Instead, the DoD should follow the same playbook it uses to seek corrections for other aspects of performance: contractual remedies included under the applicable inspection clause.[153] Inspection clauses that address other aspects of performance, including services,[154] supplies,[155] or construction,[156] allow the DoD "(1) to require contractor correction, (2) to correct the defects itself or have them corrected by another contractor, charging the contractor for the expense, (3) terminated [sic] for default, or (4) to obtain a price reduction."[157] These standard remedies provide a basic framework for consequences in cases of cybersecurity noncompliance and can be easily applied in this context.[158] Making the DoD's right to demand post-inspection corrections to cybersecurity safeguards explicit can only make obtaining these corrections easier. It can also help avoid any costs the contractor might seek to pass on to the DoD for bringing its systems into compliance.

Prominently stating that terminations are appropriate when cybersecurity requirements are not met boldly demonstrates that these requirements are an essential part of contractor performance. Tailored price adjustment language could allow the DoD to reduce the contract price by the amount of money the contractor saved by not implementing the necessary corrections, as it has done in other contexts.[159]

---

[151] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 7 tbl.2 (noting that every contractor audited showed significant cybersecurity control deficiencies).
[152] *See* May, *supra* note 131, at 47 (describing the impact of trust and legitimacy on compliance).
[153] *See* CIBINIC, JR. ET AL., *supra* note 110, at 756-61 (detailing the government's remedies for issues identified during inspections under the various inspection clauses of the FAR).
[154] *See, e.g.*, FAR 52.246-4 (2022) (regarding inspection of services-fixed-price).
[155] *See, e.g.*, FAR 52.246-3 (2022) (regarding inspection of supplies-cost-reimbursement).
[156] *See* FAR 52.246-12 (2022) (regarding inspection of construction).
[157] CIBINIC, JR. ET AL., *supra* note 109, at 756.
[158] Remedy (2), charging the contractor for corrections made to their work, is the only remedy likely inapplicable to the cyber context because we are seeking to correct the contractor's own systems. *See* CIBINIC, JR. ET AL., *supra* note 109, at 758-59.
[159] *See, e.g.*, Techni Data Labs., ASBCA 21054, 77-2 BCA ¶ 12,667 (finding the Government was entitled to an equitable adjustment reducing the contract price by $17,514 because the contractor had saved that amount by failing to correct deficiencies in its performance).

By crafting an inspection clause that clearly authorizes these standard government remedies as the situation dictates, the DoD can alleviate essentially all the concerns discussed above with existing means of enforcement. The DoD could compel correction without having to prove damages, resort to termination in every case, or rely on the FCA to address what is a very common issue that rarely requires criminal or civil judicial action.[160] Just as importantly, with remedies specifically spelled out in the contract, both contracting officers and contractors will have clear, known, predictable consequences for non-compliance, which are vital to motivating compliance going forward.

C. Meaningfully Evaluating Contractor Performance

Once the DoD's ability to inspect cybersecurity systems and act to address deficiencies is clearer, the DoD must actually evaluate contractor performance to motivate compliance and uncover systemic challenges. Meaningful evaluations can overcome the obstacles that plagued the prior self-evaluation framework and can lead to a healthier cyber environment throughout the defense industrial base.

While, as discussed above, the Government's clear right to inspect cybersecurity systems motivates compliance, that effect relies upon the possibility that the DoD will, indeed, inspect. Inspections that correctly identify issues will, for the most part, result in corrections.[161] While this sounds straightforward, relying on contracting officers and contracting officer representatives to evaluate cybersecurity requirements as part of their general contract administration duties has failed.[162] Although this was due in part to some agencies' belief that they could not access contractor systems,[163] even where access was not an issue, contracting officers and contracting officer representatives simply lacked the expertise to identify concerns.[164] An alternative attempt to move inspection responsibility outside contracting offices (by requiring what was

---

[160] There will still, however, be a place for FCA action when the facts warrant it.

[161] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 8-10 (discussing actions taken by contractors once it was discovered, and they were informed, that they had failed to implement required multifactor authentication requirements).

[162] *See* discussion *infra* Part II.B.

[163] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (discussing some agencies' beliefs that existing contract language did not allow them to review contractor cyber networks).

[164] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at 28 (stating that contracting officers and their representatives did not feel they had "the resources to review compliance").

essentially a mandatory pre-inspection via the CMMC third-party certification framework) also failed after the plan's public comments and feedback steered the DoD in a different direction.[165]

A middle ground between these approaches adds expertise to the contractor cybersecurity evaluations while continuing to rely on the local contracting office that's administering requirements: the appointment of a technical representative with cybersecurity expertise to conduct inspections and advise the contracting officer's representative. This is a need that has already been anticipated in other contexts. For example, the Department of State Acquisition Regulation (DOSAR), which is the Department of State's FAR supplement, already anticipates the need for such an individual. Part 642 of DOSAR, governing contract administration and audit services, states:

> The contracting officer may appoint a Government Technical Monitor (GTM) to assist the Contracting Officer's Representative (COR) in monitoring a contractor's performance. The contracting officer may appoint a GTM because of physical proximity to the contractor's work site, or because of special skills or knowledge necessary for monitoring the contractor's work. The contracting officer may also appoint a GTM to represent the interests of another requirements office or post concerned with the contractor's work. A GTM shall be a direct-hire U.S. Government employee.[166]

An individual with the right knowledge and responsibilities, appointed with or without the DoD's adoption of a similar provision in the DFARS,[167] is perfectly positioned to fill the knowledge gap that has

---

[165] *See About CMMC*, *supra* note 103 (announcing the withdrawal of the CMMC 1.0 framework after receiving "more than 850 public comments in response to the interim DFARS rule").

[166] DOSAR 642.271 (2020). The title "Government Technical Monitor" (GTM), as used here, references a person distinct from the contracting officer's representative. It is not, as used by some agencies in the past, an alternative means of identifying an individual with contracting officer's representative responsibilities. *See, e.g.*, U.S. DEP'T OF HOUS. & URB. DEV., HUD-1044 ASSISTANCE AWARD/AMENDMENT (1990), https://www.hud.gov/sites/documents/1044.PDF (referencing a "Government Technical Representative" in section 9).

[167] While a rule reflecting a policy position in favor of the use of GTMs would be helpful, nothing currently bars contracting officers from appointing individuals with GTM duties. *See* U.S. DEP'T OF DEF., CONTRACTING OFFICER'S REPRESENTATIVES GUIDEBOOK 15 (2021) (noting "these functions and contract surveillance are not solely the responsibility of the Contracting Officer and the COR; other individuals may have designated surveillance responsibilities").

hindered contracting officers and contracting officer representatives in the past. The DoD already employs at least 70,000 cybersecurity professionals,[168] and has a total combined information technology and cyber workforce of at least 150,000 people[169] managing an inventory spread over 5,000 locations.[170] Cybersecurity and/or information technology professionals from the DoD will almost always be located at or near the place of contract performance. These individuals can review the contractors' self-evaluations as long as contracting officers and contracting officer representatives are empowered to collaborate with them.

Utilizing existing cybersecurity and information technology experts is unlikely to impose any excessive burden on Government personnel. Inspections can occur infrequently at the Government's convenience (i.e., when personnel are available, and when inspections will not impact everyday duties), and should never take more than three hours.[171] Moreover, there should not be significant additional cost for the Government to utilize its own employees on a relatively rare basis.[172] Contractors should not face significant expenses either. Any additional costs associated with correcting deficiencies is attributable to meeting

---

[168] *See* C. Todd Lopez, *DOD Mission Big Draw for Cyber Defense Job Applicants*, U.S. DEP'T OF DEF., (Nov. 14, 2019), https://www.defense.gov/News/News-Stories/Article/Article/2017163/dod-mission-big-draw-for-cyber-defense-job-applicants (indicating that the department had 70,000 cyber professionals but intended to hire thousands more going forward).

[169] Jared Serbu, *DoD has a New Plan to Apply Enterprise-Wide Talent Management to its Cyber Workforce*, FED. NEWS NETWORK (Mar. 10, 2023, 7:11 AM), https://www.federalnewsnetwork.com/defense-news/2023/03/dod-has-a-new-plan-to-apply-enterprise-wide-talent-management-to-its-cyber-workforce/.

[170] *See* U.S. DEP'T OF DEF., DOD DIGITAL MODERNIZATION STRATEGY 7 (2019).

[171] Three hours is the estimated amount of time DoD assessors will need to conduct mid-tier level contractor assessments under the NIST SP 800-171 DoD Assessment Methodology, which was originally rolled out at the same time as CMMC 1.0. Inspections are not meant to replace assessments and should not be more in depth or take more time than standardized DoD assessments evaluating contractors who handle more sensitive information than those contractors being inspected. *See* CYBERSECURITY REQUIREMENTS RIA, *supra* note 58, at 8.

[172] Inspections should be infrequent. They are not meant to replace DoD cybersecurity assessments already in place, and there is no requirement that every contractor be inspected. To require inspections of all contractors whose cybersecurity systems have not been otherwise assessed would simply add another tier of mandatory assessments, which is not the goal of the inspection process. Instead, inspections should occur when issues are believed to exist and, in other circumstances, with enough regularity that all contractors can reasonably expect the possibility their systems will be evaluated. This corrects issues with contractors with known deficiencies, while motivating honest self-evaluations and corrections in all other contractors, who are aware of the real likelihood they will face an inspection.

existing cybersecurity requirements under the contract, not the inspection process.

Collaborating with in-house cybersecurity experts lifts the DoD over one of the last hurdles it has historically faced when evaluating cybersecurity compliance: the lack of evaluator expertise. With a path towards meaningful inspections and remedies in place, the DoD will finally have effective tools available to motivate serious compliance with cybersecurity requirements.

D. Compiling Performance Data

The DoD can expand the impact of these now-effective inspections by purposefully recording both the results and the remedial measures taken against contractors. The DoD has historically struggled with understanding, even in general terms, the scope of the industrial base's compliance with cybersecurity requirements.[173] At the same time, contractors rarely faced consequences for failing to meet cybersecurity requirements, which has limited their motivation to improve. Both these issues can be resolved in part by actively recording compliance data from the inspection in a way that is useful to the DoD.

Recording inspection data concerning cybersecurity compliance, at the individual contractor level, is relatively straightforward. The entirety of the DoD can record compliance in Contractor Performance Assessment Reporting System (CPARS)[174] performance evaluations. These performance evaluations are the DoD's mechanism for recording "Past Performance Information"[175] and are "used to communicate contractor strengths and weaknesses to source selection officials" for future decisions.[176] Including cybersecurity inspection data in these reports would immediately benefit future source selection decisions by documenting positive or negative information related to the contractor's cyber compliance. It would also significantly motivate the contractor to

---

[173] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11 (requiring a year-long investigation just to attempt to understand current challenges).
[174] CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM, https://www.cpars.gov (last visited May. 8, 2023).
[175] U.S. GEN. SERVS. ADMIN., GUIDANCE FOR THE CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS) 3 (2022), https://www.cpars.gov/documents/CPARS-Guidance.pdf.
[176] *Id.*

meet all contract requirements in order to preserve its ability to win future DoD contracts.[177]

Importantly, this can be done quickly and cheaply. Adding comments regarding cybersecurity would require essentially no additional resources; these reports are already prepared for all contracts that meet minimum criteria.[178] These comments can also be added immediately. Current regulatory guidance in FAR 42.1503 allows the past performance evaluation to include topics not specifically listed,[179] such as the failure to comply with certain contract terms and conditions.[180]

However, for CPARS comments on cybersecurity compliance to become a regular occurrence, there must be more than just the option to evaluate compliance. There must be an incentive for it to become regular practice among contracting offices. Without regularly including such comments, contractors cannot learn to expect performance evaluations, which lessens the effect of such comments on their motivation to comply, and the DoD will not have sufficient data on past performance to draw meaningful comparisons. The DoD can easily address this concern by requiring their inclusion in CMMC 2.0's rollout.[181]

Notably, inclusion will also help alleviate one of the DoD's biggest problems in addressing the cybersecurity of the defense industrial base: the inability to understand whether problems existed, and, if so, where contractors systemically struggled with compliance and how they could improve.[182] The DoD has taken several significant efforts just to gather one-time snapshots of cyber hygiene data for its use,[183] none of which can produce continuously usable data. That can change now simply by regularly compiling, sharing, and utilizing data from inspection results.

---

[177] *See* FAR 15.305 (2022) (authorizing and detailing procedures for the use of past performance information in proposal evaluations).
[178] *See* FAR 42.15 (2022) (stating when past performance evaluations shall be prepared, how to prepare them, and what contents they should contain).
[179] FAR 42.1503(b)(2)(vi) (2022).
[180] *See id.* (indicating that a contractor's "failure to report in accordance with contract terms and conditions" would be a permissible evaluation factor in a past performance evaluation).
[181] *See About CMMC*, *supra* note 103 (indicating that "[t]he Department [of Defense] intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (C.F.R.) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the C.F.R" and that "[b]oth rules will have a public comment period").
[182] *See* DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at ii (providing an overview of the struggles DoD Component contracting offices to understand the scope of cyber compliance failures amongst contractors).
[183] *See, e.g.*, DOD IG ROI-CONTRACTOR-OWNED NETWORKS, *supra* note 11, at ii (requiring a year-long study to attempt to ascertain issues with cyber compliance in the defense industrial base).

This can greatly alleviate the DoD's effort to gather reliable data as it seeks to improve its programs and understand the challenges its partners face.

IV. Conclusions

The original CMMC framework, through universal third-party assessments, sought to address chronic verification and enforcement issues that plagued the DoD's attempts to improve the cybersecurity of its contractors' networks. While real concerns led the DoD to eventually remove the third-party assessment requirement for the majority of contractors, the return to self-monitoring for those contractors, without additional changes, means that verification and enforcement concerns remain unaddressed. Without the addition of new means of verification and enforcement, it is unlikely that the new framework will lead to meaningful improvements in compliance.

The DoD must address this weakness in current plans by including a means of verifying and enforcing requirements for contractors who self-certify cybersecurity compliance alongside CMMC 2.0. The most effective and efficient way to do so is by adopting regulatory language that allows the DoD a clear means of verification through inspection, along with language providing a practical means of correction and enforcement. With access and enforcement rights clarified, the DoD will still need the appropriate resources to conduct meaningful inspections, but it can do so by utilizing the talent it already has in place. By accurately recording and utilizing inspection results, this verification and enforcement can provide a continuous means of improvement going forward. If the DoD adopts this framework, it will for the first time have a robust set of tools to identify cybersecurity issues, correct failures, and motivate compliance among its self-certifying contractors. If it does not, then the status quo, with its history of widespread noncompliance, will continue.

THIS PAGE INTENTIONALLY LEFT BLANK