Congressional Research Service
Informing the legislative debate since 1914

# Defense Acquisitions: DOD's Cybersecurity Maturity Model Certification Framework

December 18, 2020

**Congressional Research Service**
https://crsreports.congress.gov
R46643

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46643

December 18, 2020

**Heidi M. Peters**
Analyst in U.S. Defense Acquisition Policy

# Defense Acquisitions: DOD's Cybersecurity Maturity Model Certification Framework

Cybersecurity threats represented by cyberattacks and data theft have had a significant impact on the Department of Defense (DOD) and the defense industrial base (DIB). These threats have become a significant concern to policymakers due to recent alleged incidents involving the unlawful acquisition of significant quantities of sensitive defense information from DIB systems. As part of its response to these threats, DOD began work in early 2019 to develop the Cybersecurity Maturity Model Certification (CMMC) framework. This DOD-driven initiative intends to provide a "unified cybersecurity standard" for defense acquisitions and aims to use and build on existing law and regulations.

Once fully in place, the CMMC framework would establish a "verification mechanism" requiring all prime contractors and subcontractors seeking to do business with the DOD to obtain certification from accredited third-party organizations that contractors' in-house cybersecurity practices and processes meet certain standards. The DOD's CMMC framework is intended to protect *federal contract information*—or information provided by or generated under government contract not intended for public release—and to enhance security for *controlled unclassified information* generated in the course of contracted activities.

DOD anticipates fully implementing the CMMC framework over a five-year period (i.e., it may fully apply to DOD-covered contracts perhaps starting in Fiscal Year (FY) 2026, or on or after October 1, 2025). The Defense Department asserts the framework will provide increased assurance to the department that a DIB contractor can adequately protect controlled unclassified information and federal contract information at a level commensurate with the associated risk. The framework includes a system of tiered requirements based on a contract's specific cybersecurity needs. For example, *level one* requires basic cybersecurity, whereas *level five*, the highest level, entails state-of-the-art cybersecurity. DOD has asserted that the majority of defense contractors and subcontractors will require a Level 1 certification. About another 15,000 cleared defense contractors may require Level 3 certification or higher. A single contract may require different certification levels for each participating entity, depending on the specific contractual responsibilities assigned to a prime contractor and its subcontractors. On September 29, 2020, the DOD released an interim rule to begin its phase-in of the CMMC framework requirements. The interim rule took effect November 30, 2020, and the first contracts that could include CMMC requirements may be awarded in 2021.

Congress has also worked to mitigate DIB cybersecurity risks and vulnerabilities through a variety of policy initiatives, including related authorizations legislation considered by the 116th Congress (P.L. 116-92); see also provisions incorporated into the House and Senate versions of the FY2021 National Defense Authorization Act (NDAA) (H.R. 6395 and S. 4049) that could shape future development of the CMMC framework.

# Contents

Introduction ..... 1
Background ..... 1
Cybersecurity Maturity Model Certification ..... 4
Early Development ..... 8
Framework Overview ..... 9
Certification Process ..... 10
Implementation Timeline and Interim Rule ..... 12
Industry Views ..... 14
Issues for Congress ..... 15

## Figures

Figure 1. Progression of CMMC Framework Levels ..... 7
Figure 2. Comparison of CMMC Framework Views for the "Access Control" Domain ..... 10
Figure 3. Provisional DOD Phase-In Timeline for CMMC Requirements, FY2021-2025 ..... 12

## Tables

Table 1. Requirements Included in Each CMMC Level ..... 7

Table C-1. CMMC Framework, by Domains and Capabilities ..... 24

## Appendixes

Appendix A. Current Regulatory and Statutory Treatment of Cybersecurity Risk and Vulnerability Mitigation in the Defense Industrial Base ..... 17
Appendix B. NIST Special Publication 800-171 ..... 23
Appendix C. Overview of CMMC Domains and Capabilities ..... 24

## Contacts

Author Information ..... 25

# Introduction

In recent years, cybersecurity threats and attacks have become a key issue for the Department of Defense (DOD). At present an estimated 300,000 companies supply products and services to the nation's defense industrial base (DIB).[1] Concerns have been raised that some of these U.S. military contractors may pose a substantial cybersecurity risk because they currently operate with limited oversight of their internal cybersecurity controls.[2]

One effort to address cybersecurity attacks and the associated economic and national security costs to the DOD supply chain is the department's ongoing work to implement its Cybersecurity Maturity Model Certification (CMMC) framework. This initiative is designed to provide a scalable cybersecurity standard for the full spectrum of defense acquisitions.[3] Once fully implemented, with a current target date of fiscal year (FY) 2026, the framework would require all DOD prime contractors and subcontractors to receive verification through accredited third-party certification organizations that an individual organization's internal cybersecurity practices and processes meet certain standards.[4]

This report offers an overview and analysis of issues for Congress associated with the CMMC framework. This report also discusses congressional considerations related to the Defense Department's efforts to mitigate cybersecurity risks and vulnerabilities within the DIB in the performance of DOD's government contract work.

# Background

The DOD relies extensively on private companies and other entities who make up the *defense industrial base* (DIB). These suppliers provide the products and services that enable DOD's business operations and warfighting capabilities.[5] The DIB generally comprises public-sector (government-owned, government-operated) facilities; private-sector (commercial or nonprofit) companies and organizations; educational institutions; and government-owned facilities managed by corporate, academic, or nonprofit organizations (such as Sandia National Laboratories) known

[1] Connie Lee, "Vital Signs 2020: Small Businesses Concerned about New Cybersecurity Certification," *National Defense*, January 23, 2020, at https://www.nationaldefensemagazine.org/articles/2020/1/23/small-businesses-concerned-about-new-cybersecurity-certification.

[2] See for example Government Accountability Office (GAO), "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," GAO-19-128, October 9, 2018, available at https://www.gao.gov/products/GAO-19-128 and Government Accountability Office, "Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene," GAO-20-241, April 13, 2020, available at https://www.gao.gov/products/GAO-20-241, See also Department of Defense Office of Inspector General, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," DODIG-2019-105, publicly released July 25, 2019, available at https://www.dodig.mil/reports.html/Article/1916036/audit-of-protection-of-dod-controlled-unclassified-information-on-contractor-ow/.

[3] Office of the Undersecretary of Defense for Acquisition and Sustainment (OUSD(A&S)), "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020, available at https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

[4] C. Todd Lopez, "DOD to Require Cybersecurity Certification in Some Contract Bids," *DOD News*, January 31, 2020, available at https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/.

[5] See CRS In Focus IF10548, *Defense Primer: U.S. Defense Industrial Base*, by Heidi M. Peters and CRS In Focus IF11311, *Defense Primer: The National Technology and Industrial Base*, by Heidi M. Peters.

as government owned-contractor operated (GOCO) facilities.[6] The DIB entities that work with the DOD as prime contractors and subcontractors are diverse, ranging in size from small- and medium-sized businesses to some of the world's largest corporations. Together, these entities provide a wide range of products and services to the DOD, encompassing everything from complex platforms unique to the military (e.g., aircraft carriers) and highly specialized services (such as launching military satellites), to all kinds of commercial products (e.g., laptop computers and semiconductors) and routine services (e.g., information technology (IT) support).

To date, policymakers, including those in the Executive Branch and some Members of Congress, have primarily focused on mitigating related risks and vulnerabilities of the DIB through creating contractual requirements to safeguard contractor information systems that handle certain categories of federal information, or by establishing notification and reporting procedures for cybersecurity breaches. However, policymakers over the past ten years have increasingly warned about the threat of cyber attacks and data theft from the DIB, with many citing numerous news reports and congressional reports alleging the theft of significant quantities of sensitive defense information from U.S. defense contractor systems.[7] These concerns have been exacerbated by high-profile incidents such as:

- The theft of significant quantities of design data and other production-related information for the F-35 Joint Strike Fighter;[8]
- The theft of a significant quantity of data relating to submarines and underwater weaponry from a contractor working with the U.S. Navy's Naval Undersea Warfare Center; and [9]
- The findings of a 2014 Senate Armed Services Committee investigation into cyber intrusions affecting U.S. Transportation Command (TRANSCOM) contractors. The committee's investigation "identified approximately 50 successful intrusions or other cyber events … targeting TRANSCOM contractors," many of which the committee's investigators attributed to individuals associated with the Chinese government.[10]

Other government agencies such as the Government Accountability Office (GAO) and the DOD Inspector General, have highlighted widespread cybersecurity vulnerabilities in major weapons systems and a lack of DOD and DIB adherence to minimum cybersecurity best practices.[11]

---

[6] See CRS In Focus IF11466, *Defense Primer: Department of Defense Maintenance Depots*, by G. James Herrera.

[7] See, for example, Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies," *The Washington Post*, May 27, 2013; Helene Cooper, "Chinese Hackers Steal Unclassified Data From Navy Contractor", *The New York Times*, June 18, 2018; and Gordon Lubold and Dustin Voltz, "Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts," *The Wall Street Journal*, March 12, 2019..

[8] See David Alexander, "Theft of F-35 design data is helping U.S. adversaries – Pentagon," *Reuters*, June 19, 2013 and Siobhan Gorman et al., "Computer Spies Breach Fighter Jet Project," *Wall Street Journal*, April 21, 2009.

[9] U.S. Congress, House Committee on Armed Services, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, conference report to accompany H.R. 5515, 115th Cong., 2nd sess., July 23, 2018, H.Rept. 115-863, pp. 1053-1054. See also Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *The Washington Post*, June 8, 2018, available at 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.

[10] U.S. Congress, Senate Committee on Armed Services, *Inquiry Into Cyber Intrusions Affecting U.S. Transportation Command Contractors*, 113th Cong., 2nd sess., September 18, 2014, S.Rept. 113-258.

[11] Government Accountability Office (GAO),, "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," GAO-19-128, October 9, 2018, available at https://www.gao.gov/products/GAO-19-128 and

Congress has echoed these concerns in numerous hearings and public statements—for example, during a February 2019 hearing of the House Armed Services Committee Subcommittee on Intelligence, Emerging Threats, and Capabilities, Representative James Langevin said that the "thefts of DOD data from contractors and the security of weapons systems themselves are both challenges that we absolutely have to address."[12] More recently, the Senate Report (S.Rept. 116-48) for S. 1790, the FY2020 National Defense Authorization Act (NDAA), called for prime contractors to be held "responsible and accountable for securing Department of Defense technology and sensitive information and for delivering products and capabilities that are uncompromised" by cybersecurity vulnerabilities.[13]

Congress has worked to mitigate perceived and verified DIB cybersecurity risks and vulnerabilities through a variety of policy initiatives, including the following selected response mechanisms identified by CRS:

- Requiring the DOD to issue or modify internal acquisition procedures and policies, or modifying DOD-specific acquisition authorities;[14]
- Establishing procedures—and requiring DOD to establish procedures—for information sharing, notification, and reporting requirements related to cybersecurity breaches and loss of certain types of information for both the DOD and certain categories of defense contractors;[15]
- Restricting procurement of supplies or services from certain sources;[16]
- Establishing advisory bodies or councils, both within the DOD and across the whole of federal government;[17]

---

Government Accountability Office, "Cybersecurity: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene," GAO-20-241, April 13, 2020, available at https://www.gao.gov/products/GAO-20-241, See also Department of Defense Office of Inspector General, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," DODIG-2019-105, publicly released July 25, 2019, available at https://www.dodig.mil/reports.html/Article/1916036/audit-of-protection-of-dod-controlled-unclassified-information-on-contractor-ow/.

[12] House Armed Services Committee Subcommittee on Intelligence, Emerging Threats, and Capabilities, "Department of Defense Information Technology, Cybersecurity, and Information Assurance," hearing transcript, February 26, 2019. See also Senate Armed Services Committee Subcommittee on Cybersecurity, "Defense Industrial Base Cybersecurity Policy," hearing held April 10, 2019.

[13] U.S. Congress, Senate Committee on Armed Services, *National Defense Authorization Act for Fiscal Year 2020*, report to accompany S. 1790, 116th Cong., June 11, 2020, S.Rept. 116-48, p. 306.

[14] Other DOD policy guidance with respect to defense cybersecurity and information assurance; risk management frameworks for DOD information technology; counterfeit parts in the defense supply chain; and related topics is outside of the scope of this report. For a high-level overview of applicable cybersecurity policies, see DOD Chief Information Officer, "Policies: Defend against Cyber Attack," available at https://dodcio.defense.gov/Library/.

[15] For example, 10 U.S.C. §393 requires the Secretary of Defense to establish procedures mandating reporting to a designated DOD component when certain types of covered networks or information systems operated by cleared defense contractors are successfully penetrated. See **Appendix A** for a more in-depth discussion of the reporting requirements.

[16] See Section 1655 of the FY2019 NDAA (P.L. 115-232), which established that the DOD may not use a product, service, or system procured or acquired relating to information or operational technology, cybersecurity, an industrial control system, or weapons system provided by a person unless that person makes a series of disclosures regarding potential obligations to foreign governments; see also Section 1634 of the FY2018 NDAA (P.L. 115-91), which established a federal government-wide prohibition on the use of products and services developed or provided by Kaspersky Lab, as well as Section 1656 of the FY2018 NDAA (see 10 U.S.C. §491 note).

[17] See for example, Section 202 of P.L. 115-390, which amended Title 41 (41 U.S.C. §1321-1328) to establish a new Federal Acquisition Security Council.

- Authorizing the DOD to run related pilot programs; and [18]
- Requiring the DOD to produce certain reports, assessments, frameworks, or strategy documents.[19]

For a more in-depth discussion of selected current statutory and regulatory requirements related to the mitigation of DIB cybersecurity risks and vulnerabilities—both broadly applicable to federal procurement and specifically to the DOD—see **Appendix A**.

# Cybersecurity Maturity Model Certification

Although the DOD has broad latitude to improve the cybersecurity of government-owned and operated information systems, the department has more limited mechanisms to influence the behaviors—such as maintaining internal cybersecurity practices that adhere to certain minimum standards—of the approximately 300,000 private-sector companies and organizations that comprise the majority of the DIB. Some progress in improving DIB cybersecurity has been achieved through the 2016 introduction of regulatory requirements that are applicable to most DOD contracts, barring those solely for commercial-off-the-shelf items, which mandate contractor adherence to guidelines introduced by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.[20] See **Appendix A** for a discussion of the applicable regulatory requirements and **Appendix B** for a discussion of the NIST guidelines.

Nevertheless, some observers and DOD officials have increasingly viewed cybersecurity as foundational to the procurement process and advocated for a mechanism to "verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level."[21] In keeping with this viewpoint, in early 2019 the DOD began to develop its Cybersecurity Maturity Model Certification (CMMC) framework, which it expects to implement

[18] See for example, Section 215 of the FY2011 NDAA (P.L. 111-383) which authorized the Secretary of Defense to support or conduct pilot programs on cybersecurity with respect to certain defined areas, including processes for securing the supply chain.

[19] See for example, Section 1648 of the FY2020 NDAA (P.L. 116-92) which required the Secretary of Defense to develop a consistent, comprehensive framework to enhance cybersecurity for the U.S. DIB, to include certain required elements, specific matters for consideration, and consultation with designated stakeholders. Section 1645 of the FY2020 NDAA requires the Principal Cyber Advisor to the Secretary of Defense and DOD Chief Information Officer to submit a classified annual report through FY2023. The report is required to detail cyberattacks and intrusions in the previous year carried out by agents or associates of the People's Republic of China, the Russian Federation, the Islamic Republic of Iran, and the Democratic People's Republic of Korea against information systems of the DOD or any DOD contractor that works on sensitive U.S. military technology.

[20] See Shay D. Assad, Director, Defense Pricing/Defense Procurement and Acquisition Policy, "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," memorandum, September 21, 2017, available at https://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf.

[21] In August 2019, Special Assistant for Cyber to the Assistant Secretary of Defense for Acquisition (ASD(A)) Katie Arrington reportedly stated that: "[i]t doesn't matter how much I pay for something if it's already been [stolen]. … If I'm worried about getting it on time, but by the time I get it delivered to me it's worthless, why am I worrying about the schedule? Yeah, I wanted it to perform at this capacity, but if my adversaries already have it, they're outperforming me before I get there." See Derek B. Johnson, "Contractors Have Questions about DOD's Cyber Requirements," *FCW,* August 12, 2019, available at https://fcw.com/articles/2019/08/12/dod-contractor-cyber-johnson.aspx. See also OUSD(A&S), "Cybersecurity Maturity Model Certification (CMMC) Model v.1.0," briefing slides, January 31, 2020, available at https://www.acq.osd.mil/cmmc/docs/CMMC_v1.0_Public_Briefing_20200131_v2.pdf and OUSD(A&S), "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020, available at https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

fully by Fiscal Year (FY) 2026.[22] Building on the NIST requirements, the CMMC framework is intended to provide a "unified cybersecurity standard" for defense acquisitions building on existing law and regulations.[23] Once fully implemented, the framework would use the DOD's contractual leverage to require all prime contractors and subcontractors seeking to do business with the department to obtain verification from accredited third-party certification organizations that in-house cybersecurity practices and processes meet certain standards.[24]

The CMMC framework is intended to ensure basic protection of *federal contract information*—or information provided by or generated for the government under contract that is not intended for public release—and enhanced security for *controlled unclassified information* generated in the course of contracted activities.[25]

**Controlled Unclassified Information—What is It?**

The term *controlled unclassified information* (CUI) generally refers to certain types of information produced or accessed in the course of U.S. government activities that require safeguarding or disseminating controls pursuant to applicable law, regulations, and government-wide policies.

CUI is not considered classified information under Executive Order 13526 or the Atomic Energy Act, as amended.[26] Examples of CUI include patent applications, technical defense information, and DOD critical infrastructure security information.[27] The CUI categorization was established by Executive Order 13556 in 2010; the National Archives and Records Administration (NARA) is the Executive Agent responsible for implementing the order and overseeing agency compliance.[28] DOD policy with respect to CUI is established by DOD Instruction 5200.48, "Controlled Unclassified Information (CUI)."[29]

[22] Department of Defense, "Press Briefing by Under Secretary of Defense for Acquisition & Sustainment Ellen M. Lord, Assistant Secretary of Defense for Acquisition Kevin Fahey, and Chief Information Security Officer for Acquisition Katie Arrington," January 31, 2020, available at https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/.

[23] OUSD(A&S), "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020, available at https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf. See also OSD(A&S) Industrial Policy, "Fiscal Year 2019 Industrial Capabilities: Report to Congress," June 23, 2020, available through https://www.businessdefense.gov/resources/.

[24] C. Todd Lopez, "DOD to Require Cybersecurity Certification in Some Contract Bids," *DOD News*, January 31, 2020, available at https://www.defense.gov/Explore/News/Article/Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/.

[25] As defined in Federal Acquisition Regulation (FAR) Subpart 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," as added June 2016.

[26] Executive Order 13526, issued in 2009 by President Barak Obama, modified the existing U.S. government system for classifying, safeguarding, and declassifying national security information. See Executive Office of the President, "Executive Order 13526 of December 29, 2009: Classified National Security Information," 75 *Federal Register* 707-731, January 5, 2010. The Atomic Energy Act (Chapter 23 of Title 42, U.S. Code) sets government-wide policy for classifying, safeguarding, and declassifying *Restricted Data* (i.e., information related to atomic energy, defined for the purposes of the Act as all forms of energy released in the course of nuclear fission or nuclear transformation).

[27] National Archives, "Controlled Unclassified Information (CUI)," available at https://www.archives.gov/cui/registry/category-list; see also Executive Order 13556, "Controlled Unclassified Information," 75 *Federal Register* 68675, November 4, 2010 and see also NARA Information Security Oversight Office, "Controlled Unclassified Information," 81 *Federal Register* 63323, September 14, 2016.

[28] National Archives, "Controlled Unclassified Information (CUI)," available at https://www.archives.gov/cui.

[29] DOD Instruction 5200.48, "Controlled Unclassified Information (CUI)," Office of the Under Secretary of Defense for Intelligence and Security, March 6, 2020, available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF.

The CMMC framework will only is to apply to contracts valued at greater than the micro-purchase threshold (generally $10,000).[30] Only vendors solely providing commercial-off-the-shelf products (as defined by 41 U.S.C. §104) are to be exempted from the requirement; the DOD is not anticipating that waivers will be provided to companies unable to meet the requirements of the CMMC framework.[31] In a press briefing on December 10, 2019, Under Secretary of Defense for Acquisition and Sustainment Ellen M. Lord elaborated:

> At this point, I don't rule anything out, but I'm not envisioning waivers. I am envisioning the primes and the industry associations and the government with industrial policy, really working as kind of the help desk, the help agent, enabling these companies to be compliant with a lot of support.[32]

The Defense Department asserts that the CMMC framework will provide increased assurance to the department that a DIB contractor can adequately protect CUI and federal contract information at a level commensurate with the associated risk. In order to do so, and in recognition that "[cyber]security is not one size fits all," the CMMC framework includes a system of tiered requirements depending on a contract's specific cybersecurity needs, with a *level one* requirement mandating basic cybersecurity processes and practices, scaling up to *level five* requirements necessitating state-of-the-art cybersecurity (see **Figure 1**).[33] Each level is additive, with higher progression on the scale also encompassing all requirements of previous levels.

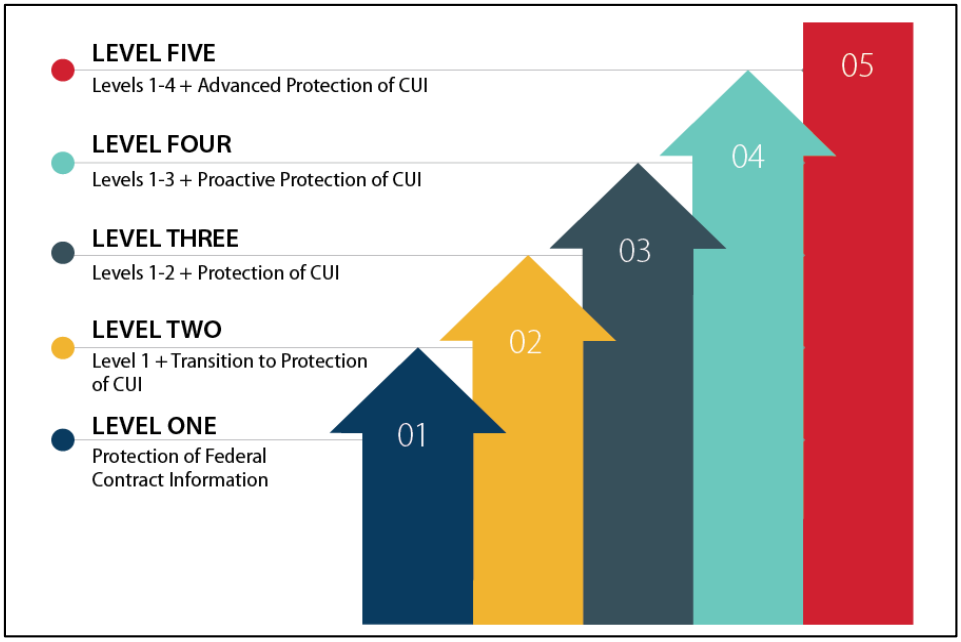
[30] Defense Acquisition Regulations System, Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020. As of June 20, 2018, the micro-purchase threshold, which applies to government purchases by the Defense Department or other federal agencies was raised from $3,000 to $10,000.

[31] See Frequently Asked Question (FAQ) #19, "My Organization Does Not Handle Controlled Unclassified Information (CUI). Do I Have to be Certified Anyway?" available at https://www.acq.osd.mil/cmmc/faq.html. See also Jackson Barnett, "CMMC Won't Apply to Commercial-Off-The-Shelf Suppliers, DOD Website Shows," *Fedscoop*, May 5, 2010, available at https://www.fedscoop.com/cmmc-exemption-cots-suppliers/.

[32] Department of Defense, "Under Secretary of Defense for Acquisition & Sustainment Ellen Lord Press Briefing on Defense Acquisition," transcript, December 10, 2019, available at https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2037206/under-secretary-of-defense-for-acquisition-sustainment-ellen-lord-press-briefin/.

[33] Remarks by Katie Arrington, Special Assistant for Cyber to the ASD(A) and Chief Information Security Officer for Acquisition, DOD press briefing, January 31, 2020, available at https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2072073/press-briefing-by-under-secretary-of-defense-for-acquisition-sustainment-ellen/.

**Figure 1. Progression of CMMC Framework Levels**




**Source:** CRS adaptation of Figure 3, "CMMC Levels and Associated Focus," Office of the Under Secretary of Defense for Acquisition and Sustainment, "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020.

The DOD has asserted that the majority of defense contractors and subcontractors will require Level 1 certification, which encompasses the NIST SP 800-171 requirements, with approximately 15,000 *cleared defense contractors* requiring the enhanced cybersecurity processes and practices associated with the Level 3 certification or higher levels.[34] A single contract may require a different certification level for each participating entity, dependent on the specific contractual responsibilities and tasks assigned to a prime contractor and subcontractors.

**Table 1. Requirements Included in Each CMMC Level**

| Level | Description |
|---|---|
| 1 | 15 basic safeguarding requirements from FAR clause 52.204–21 |
| 2 | Consists of 65 security requirements from NIST SP 800–171 as implemented via DFARS clause 252.204–7012, 7 CMMC practices, and 2 CMMC processes. Intended as an optional intermediary step for contractors as part of their progression to Level 3. |
| 3 | All 110 NIST SP 800–171 security requirements, 20 CMMC practices and 3 CMMC processes |
| 4 | All 110 NIST SP 800–171 security requirements, 46 CMMC practices and 4 CMMC processes |
| 5 | All 110 NIST SP 800–171 security requirements, 61 CMMC practices and 5 CMMC processes |

**Source:** Defense Acquisition Regulations System (DARS), Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020.

[34] CRS conversation with DOD officials, June 23, 2020. A *cleared defense contractor*, as defined in the Code of Federal Regulations (32 C.F.R. §236.2), is a "private entity granted clearance … to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of DOD."

The Defense Department has indicated that a certification will be valid for three years.[35] The full cost associated with achieving a specific certification level has not yet been confirmed; however, DOD officials have indicated that some costs for expenses associated with implementing cybersecurity processes and practices exceeding those necessary to satisfy NIST SP 800-171 requirements may be considered *allowable* for certain types of contracts.[36] An *allowable cost* in terms of federal contracting is, broadly speaking, costs that are reasonable and allocable to the contract (i.e., chargeable to the U.S. government).[37]

## Early Development

In June 2019, DOD officials publicly confirmed that a defense industry-wide standard was under development that would further authenticate the successful implementation of certain cybersecurity requirements and best practices by entities seeking to do business with the Defense Department.[38]

### Industry Standards—What Are They?

An *industry standard* can be understood as agreed-on "common and repeated use of rules, conditions, guidelines, or characteristics for products or related processes and production methods, and related management systems practices" used within a particular industry to ensure safety, uniformity, and reliability.[39] Standards can be "developed or adopted by domestic and international voluntary consensus standard-making bodies" that bring together industry representatives and stakeholders to develop and periodically update the standard as processes and methods evolve.[40] Within the United States, most standards development occurs through private sector organizations that serve as voluntary consensus standard-making bodies, such as the American National Standards Institute (ANSI).[41]

A company can obtain *certification* that it meets particular standards, such as cybersecurity standards, by undergoing an assessment provided by an independent third-party certification entity. This assessment determines if the product, service or system in question meets the requirements set forth in the standard. Entities providing these assessments can be *accredited* to do so by an independent organization—commonly referred to as an accreditation body—that ensures each certification entity within its purview is capable of evaluating adherence to the requirements of the standard(s) in question.

[35] See FAQ #15, "How Often Does My Organization Need to be Reassessed?," available at https://www.acq.osd.mil/cmmc/faq.html.

[36] CRS correspondence with OUSD(A&S)/OCISO(A&S), November 17, 2020; see Jason Miller, "Why DoD's decision to make cybersecurity an 'allowable cost' matters," *Federal News Network,* June 17, 2019, available at https://federalnewsnetwork.com/reporters-notebook-jason-miller/2019/06/why-dods-decision-to-make-cybersecurity-an-allowable-cost-matters/ and FAQ #11, "How Much Will CMMC Certification Cost?" available at https://www.acq.osd.mil/cmmc/faq.html.

[37] See Federal Acquisition Regulation (FAR) FAR Part 31.

[38] Remarks by Katie Arrington, "Defense Acquisition: Cybersecurity Maturity Model," as delivered at the 2019 Federal Acquisition Conference, June 13, 2019; see briefing slides as made available through *Inside Defense,* available at https://insidedefense.com/sites/insidedefense.com/files/documents/2019/jun/06132019_sup.pdf.

[39] As defined in White House Office of Management and Budget Circular A-119, "Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities," revised January 27, 2016, available at https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A119/revised_circular_a-119_as_of_1_22.pdf.

[40] As defined in Federal Acquisition Regulation (FAR) Subpart 2.1, "Definitions."

[41] NIST notes that ANSI does not actually create standards; rather "it administers and coordinates the activities of the U.S. private sector voluntary standardization system." See, Karen A. Scarfone, Daniel R. Benigni, and Timothy Grance, *Cyber Security Standards,* NIST, June 15, 2009, p. 5, available at https://www.nist.gov/publications/cyber-security-standards.

The full CMMC framework, released in January 2020, was developed through engagement by the Defense Department with stakeholders and industry partners, as well as with technical assistance provided by the Johns Hopkins University Applied Physics Laboratory (APL), a DOD university affiliated research center, and the Carnegie Mellon University Software Engineering Institute (SEI), a federally funded research and development center.[42] The CMMC framework incorporates guidelines derived from NIST SP 800-171, as well as cybersecurity models developed by other national and international standards-setting bodies and other entities.[43]

## Framework Overview

The CMMC framework is intended to assess the relative *maturity,* or "current level of capability … of [an entity's] processes, practices, and methods" for ensuring the protection of CUI and federal contract information in carrying out activities under contract to the DOD.[44] In order to do so, it uses a *maturity model* framework, defined as a "set of characteristics, attributes, indicators, or patterns that represent capability and progression" with progression measured by an increasing scale of tiered requirements.[45]

DOD uses two main taxonomic mechanisms to organize the interrelated requirements of the CMMC framework. The first centers on *domains*, or high-level groupings of cybersecurity requirements (e.g., control of system access). Each domain includes *practices*, framed as the relative institutionalization status of an entity's approach to cybersecurity (e.g., setting system access controls versus having documented procedures for setting system access controls), and implemented *processes*, framed as specific tasks required to carry out an overarching practice (e.g., using multifactor authentication to limit system access).[46]

The DOD also provided "additional structure" to the CMMC framework by mapping the CMMC domains against *capabilities*, framed as overarching responsibilities (e.g., limiting system access to authorized users).[47] Each capability encompasses specific institutionalized cybersecurity *practices* (see **Appendix C** for a full listing of the domains and capabilities included in the

[42] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020.

[43] Some elements of the CMMC framework include standards developed by the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) and the United Kingdom's National Cyber Security Centre. See ACSC, "Essential Eight Maturity Model," overview, July 2019, available at https://www.cyber.gov.au/sites/default/files/2019-07/PROTECT%20-%20Essential%20Eight%20Maturity%20Model%20%28July%202019%29_0.pdf and National Cyber Security Centre, "Cyber Essentials," available at https://www.ncsc.gov.uk/cyberessentials/overview. In public remarks, Undersecretary of Defense for Acquisition and Sustainment Ellen Lord reportedly also indicated that U.S. partners and allies had expressed interest in the CMMC framework, raising the possibility that the standard could become a shared requirement for defense cooperation partnerships and international collaboration. ("The CMMC team is working with multiple countries, including Canada, the U.K., Denmark, Italy, Australia, Singapore, Sweden, Poland and the E.U. cybersecurity body … All of these countries and groups acknowledged the challenge we have with cybersecurity … They're looking at what is the most efficient and effective way to secure their industrial base, and there are significant conversations about perhaps adopting our CMMC. So, more to come.") See Tony Bertuca, "Lord Says U.S. Allies Interested in Adopting CMMC Standards," *InsideDefense*, March 4, 2020, available at https://insidedefense.com/daily-news/lord-says-us-allies-interested-adopting-cmmc-standards.

[44] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Cybersecurity Maturity Model Certification," version 1.02, p. 3, March 18, 2020.

[45] Office of the Under Secretary of Defense for Acquisition and Sustainment, "Cybersecurity Maturity Model Certification," version 1.02, p. 3, March 18, 2020.

[46] OUSD(A&S), "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020.

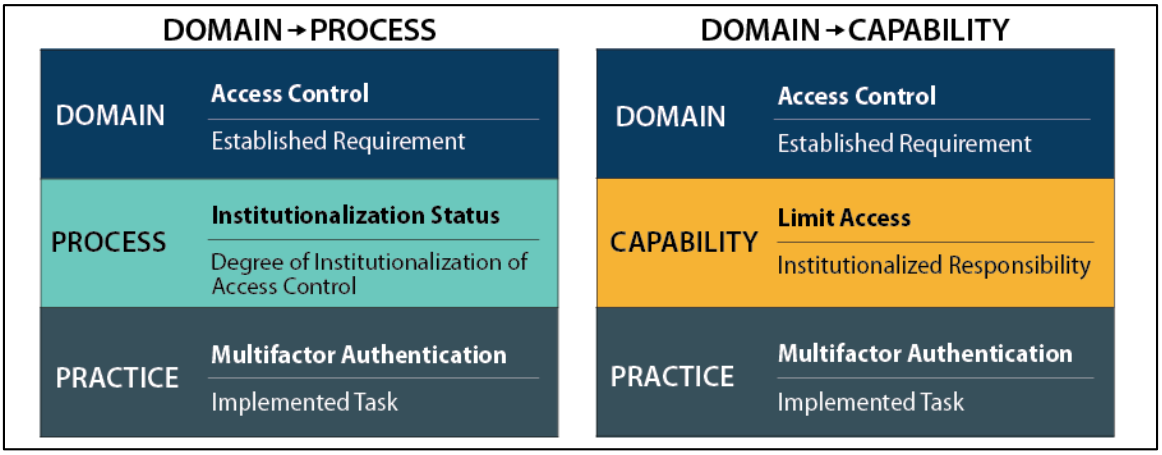
[47] OUSD(A&S), "Cybersecurity Maturity Model Certification," version 1.02, p. 3, March 18, 2020.

CMMC framework).[48] For example, the domain "Access Control" includes four specific capabilities:

- establish system access requirements;
- control internal system access;
- control external system access; and
- limit data access to authorized users and system processes.[49]

See **Figure 2** for a comparison of the two CMMC framework views for the "Access Control" domain.

**Figure 2. Comparison of CMMC Framework Views for the "Access Control" Domain**




**Source:** CRS illustration adapting information presented in Office of the Under Secretary of Defense for Acquisition and Sustainment, "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020.

## Certification Process

The CMMC framework, once implemented, would require all prime contractors and subcontractors seeking to do business with the DOD to obtain verification of a contractually applicable CMMC level from accredited third-party certifiers (*assessors*) or third-party certification organizations (*CMMC third-party assessment organization* [C3PAO]). Contracting officers will are to be required to use the Supplier Performance Risk System (SPRS), an online tool that allows the DOD to collect and review suppliers' past performance information, to verify that an entity's "CMMC certification is current and meets the required level" prior to making a contract award.[50] An accreditation body—the *Cybersecurity Maturity Model Certification Accreditation Body* (CMMC-AB)—will is to carry out the actual process of training and accrediting individual assessors and assessment organizations.[51]

[48] OUSD(A&S), "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020.

[49] OUSD(A&S), "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020.

[50] Defense Acquisition Regulations System (DARS), Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020. See also Supplier Performance Risk System (SPRS), available at https://www.sprs.csd.disa.mil/.

[51] See Memorandum of Understanding (MOU) between the Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) and Cybersecurity Maturity Model Certification

CMMC-AB is a 501(c)(3) nonprofit organization independent of the DOD to "[manage] and [oversee] CMMC accreditation, certification, approval, training, and assessment processes."[52] CMMC-AB is intended to achieve "self-sustaining" operations, with funding for the organization's operations generated by its provision of training and accreditation services.[53] In turn, the DOD has created the CMMC Office, which is to work with the CMMC-AB, as well as maintain and update the CMMC framework in order to "incorporate changes in cybersecurity requirements and threats."[54] In March 2020, the Under Secretary of Defense for Acquisition and Sustainment and the Chairman of the CMMC-AB signed a memorandum of understanding (MOU) to formalize the relationship.[55]

DOD officials have argued that setting up an independent accreditation body allows additional flexibilities—related in a narrow sense to resources and budgeting, as well as more broadly in terms of effecting the "cultural shift" represented by the CMMC framework—that would not be available to a comparable body set up as a new DOD component, or to an existing DOD component (such as the Defense Contract Management Agency) granted an expanded charter of operations. As noted in a June 2020 press report:

> Even though [the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)] does similar work to the AB and has been doing an "amazing job," [a DOD official] said it could not have been the AB or built out to run CMMC. "We couldn't do this in the DOD," [the DOD official] said … "[W]e don't have the money or the resources in our defense budget" to do what the AB must do.[56]

Some observers have pointed out that the CMMC-AB, in its current form, largely relies on volunteer work and lacks a dedicated funding stream.[57] Controversy surrounding a sponsorship program proposed by the CMMC-AB—potentially as a means of generating short-term cash flow—together with policy disputes may have contributed to the resignation of the first CMMC-AB Chairman and other CMMC-AB volunteers.[58] While some consider these factors to be

---

Accreditation Body, Inc. (CMMC-AB), signed March 2020, available at https://assets.documentcloud.org/documents/6935675/CMO001673-20-CMMC-AB-MOU-Fully-Executed-20200323.pdf.

[52] Memorandum of Understanding (MOU) between the Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) and Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB), signed March 2020, p. 2. See also CMMC-AB, "OSC – Organizations Seeking Certification", available at https://www.cmmcab.org/osc-lp and Jackson Barnett, "Here's What's in the CMMC Accreditation Body's Memo of Understanding" *Fedscoop*, June 3, 2020, available at https://www.fedscoop.com/cmmc-memorandum-of-understandin-iso-standards/.

[53] MOU between OUSD(A&S) and CMMC-AB, signed March 2020, p. 5.

[54] MOU between OUSD(A&S) and CMMC-AB, signed March 2020, p. 3.

[55] MOU between OUSD(A&S) and CMMC-AB, signed March 2020, p. 7.

[56] Jackson Barnett, "The DOD Wants Better Cybersecurity for Its Contractors. The First Steps Haven't Been Easy," *Fedscoop*, June 23, 2020, available at https://www.fedscoop.com/cmmc-dod-cybersecurity-requirments-contractors-timeline/. Barnett reported that the CMMC-AB "recently started soliciting advice from the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)," which "already does spot-assessments of contractors after cybersecurity incidents and since May has advised the board."

[57] Jackson Barnett, "The DOD Wants Better Cybersecurity for Its Contractors. The First Steps Haven't Been Easy," *Fedscoop*, June 23, 2020.

[58] Jackson Barnett, "Exclusive: CMMC board ousts chairman and other top member," *Fedscoop*, September 16, 2020, available at https://www.fedscoop.com/cmmc-ab-ousts-chairman-ty-schieber-and-mark-berman/; see also Jackson Barnett, "CMMC board offers questionable 'partner program,' but quickly backtracks," *Fedscoop*, September 9, 2020, available at https://www.fedscoop.com/cmmc-offers-partner-program-but-quickly-backtracks/ and Jackson Barnett, "CMMC board faces 'passionate' internal turmoil over new contract with DOD," *Fedscoop*, July 28, 2020, available at https://www.fedscoop.com/cybersecurity-maturity-model-certification-cmmc-issues-ab/.

temporary constraints that will be alleviated as the Accreditation Body's operations continue, others raise the potential for unintended consequences that might result from volunteers working to establish a complex bureaucratic entity that may operate at a national scale in perpetuity, especially as the CMMC-AB continues to incur debt and obligations.[59]

## Implementation Timeline and Interim Rule

On September 29, 2020, the DOD released an interim rule to begin including the CMMC framework in covered DOD contracts; the interim rule proposes a phase-in of the CMMC framework over time, anticipating its full implementation beginning in Fiscal Year (FY) 2026 (i.e., those contracts starting on or after October 1, 2025).[60]

**Figure 3. Provisional DOD Phase-In Timeline for CMMC Requirements, FY2021-2025**

as of November 2020

| Total Number of New Prime Contracts Awarded Each Year with CMMC Requirement | | | | |
|---|---|---|---|---|
| FY21 | FY22 | FY23 | FY24 | FY25 |
| 15 | 75 | 250 | 479 | 479 |

| | Total Number of Prime Contractors and Sub-Contractors with CMMC Requirement | | | | |
|---|---|---|---|---|---|
| | FY21 | FY22 | FY23 | FY24 | FY25 |
| Level 1 | 899 | 4,490 | 14,981 | 28,714 | 28,709 |
| Level 2 | 149 | 749 | 2,497 | 4,786 | 4,785 |
| Level 3 | 452 | 2,245 | 7,490 | 14,357 | 14,355 |
| Level 4 | 0 | 8 | 16 | 24 | 28 |
| Level 5 | 0 | 8 | 16 | 24 | 28 |
| Total | 1,500 | 7,500 | 25,000 | 47,905 | 47,905 |

**Source:** Department of Defense, "Securing the DOD Supply Chain: Cybersecurity Maturity Model Certification," presentation slides, October 2020.

The interim rule introduces a new Defense Federal Acquisition Regulation Supplement (DFARS) subpart, as well as accompanying solicitation and contract clauses. As currently drafted, the new DFARS Subpart 204.75 would require contracting officers to use the Supplier Performance Risk System (SPRS), an online tool that allows DOD to collect and review suppliers' past performance information, to verify that an entity's "CMMC certification is current and meets the required

[59] Jackson Barnett, "The DOD Wants Better Cybersecurity for Its Contractors. The First Steps Haven't Been Easy," *Fedscoop*, June 23, 2020; see also Frank Kendall, "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May," *Forbes*, April 29, 2020, available at https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certificationan-idea-whose-time-has-not-come-and-never-may/#3282ff033bf2.

[60] Defense Acquisition Regulations System, Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020.

level" prior to making a contract award.[61] Contractors would be responsible for adding CMMC assessment results to the SPRS tool.

The interim rule also amends DFARS Subpart 204.73, and introduces new related DFARS solicitation and contract clauses.[62] The amendments to DFARS Subpart 204.73 introduce new requirements for contracting officers to also verify in SPRS prior to contract award if a current (not older than three years) self-assessment of the offeror's implementation of requirements detailed in NIST SP 800-171 is available.[63] The Defense Department asserts that this change will allow the department to "assess contractor implementation of [the NIST SP 800-171] requirements as the Department transitions to full implementation of the CMMC" framework.[64] The interim rule specifies that, until September 30, 2025, the relevant CMMC solicitation and contract clauses should be used in approved contracts, including contracts for commercial items conducted under streamlined FAR Part 12 procedures, if the associated requirement document or statement of work requires a contractor to attain a specific CMMC level.[65] During this period, the Office of the Under Secretary of Defense for Acquisition and Sustainment must provide approval for the inclusion of such CMMC requirements.[66]

The interim rule took effect November 30, 2020. In advance of the effective date of the interim rule, the DOD has worked with departmental components and the CMMC-AB to "conduct risk reduction activities to include mock CMMC assessments, tabletop exercises, and training for candidate provisional assessors."[67] The DOD has also asked the military departments, as well as the DOD components and field activities, to nominate a total of 15 upcoming contracts that are expected to be awarded in 2021 that could include CMMC requirements in the accompanying requests for solicitations and request for proposals.[68]

---

[61] Defense Acquisition Regulations System (DARS), Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020. See also Supplier Performance Risk System (SPRS), available at https://www.sprs.csd.disa.mil/.

[62] These clauses serve to operationalize the requirements introduced by the CMMC framework. For example, DFARS Clause 252.204-7021, which is to be included in all solicitations, contracts, delivery orders, and task orders (barring those only for COTS items), requires a contractor to "maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract or other contractual instruments; and include the requirements of the clause in all subcontracts or other contractual instruments." See DARS, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020.

[63] DARS, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020. See also NIST SP 800-171 DOD Assessment Methodology, Version 1.2.1, June 24, 2020, available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf.

[64] DARS, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020.

[65] DARS, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020.

[66] DARS, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020.

[67] CRS correspondence with OUSD(A&S)/OCISO(A&S), November 17, 2020. See also CMMC Accreditation Body, "CMMC-AB Board Announces Major Milestone," September 16, 2020, available at https://www.cmmcab.org/nr-6-cmmc-ab-board-announces-major-milestone; see also Jackson Barnett, "Will there be enough CMMC assessors to certify all DOD contractors?," *Fedscoop*, October 21, 2020, available at https://www.fedscoop.com/cybersecurity-maturity-model-certificationcmmc-assessors-accreditation/.

[68] See Sara Friedman, "DOD to incorporate CMMC requirements into 15 Pentagon contracts in year one," *Inside*

## Industry Views

While generally expressing support for "CMMC's underlying vision and plan" for establishing a unified cybersecurity standard for DOD acquisition, industry organizations and observers have raised numerous questions regarding DOD's implementation of the CMMC framework.[69] Particular concern has centered on the following issue areas.

- DOD has proposed an aggressive phase-in of CMMC requirements, with the number of contractors anticipated to need approval under the CMMC framework projected to roughly quintuple between FY2021 and FY2022 (from 1,500 to 7,500) alone.[70] As of October 2020, less than 100 assessors had been granted "provisional" status, leading some to question whether an adequate number of individual assessors and assessment organizations will be in place to maintain DOD's notional schedule.[71]
- DOD asserts that the five-year phase-in of CMMC requirements is "intended to minimize the financial impacts to the industrial base, especially small entities" as such entities are defined by the Regulatory Flexibility Act (5 U.S.C. §601 et seq.).[72] While DOD has provided an analysis of estimated costs associated with a small entity implementing each level of the CMMC framework, this analysis may not adequately encompass all associated costs, such as the ongoing depreciation and ultimate replacement of necessary hardware and software; increases in hourly wages and benefits costs for employees, coupled with staff attrition and replacement; and the likelihood of direct assessment costs increasing over time.[73] Some have accordingly questioned if DOD has adequately considered the ultimate financial impact of CMMC on all levels of the DIB, as well as the cost realism of its estimates.
- As discussed in the overview of the CMMC "Certification Process," some have questioned the role and ultimate influence of the CMMC-AB on the CMMC process.

---

*Defense*, October 22, 2020, available at https://insidedefense.com/daily-news/dod-incorporate-cmmc-requirements-15-pentagon-contracts-year-one.

[69] See, for example, letter to the Office of the Under Secretary of Defense for Acquisition & Sustainment from the National Defense Industrial Association, "Re: Industry Questions on CMMC Implementation," October 8, 2020, available at https://www.ndia.org/-/media/sites/ndia/policy/blog/documents/cmmc-outstanding-questions-fall-2020.ashx?la=en. See also Information Technology Industry Council (ITI), letter to the Department of Defense, "RE: DFARS Case 2019-D041," November 30, 2020, available at https://www.itic.org/documents/public-sector/ITICommentsonDFARSCase2019-D041CMMC.pdf.

[70] Katie Arrington, "Securing the DOD Supply Chain: Cybersecurity Maturity Model Certification," presentation slides, November 2020.

[71] Jackson Barnett, "Will there be enough CMMC assessors to certify all DOD contractors?" *Fedscoop*, October 21, 2020.

[72] DARS, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020, p. 61510.

[73] DARS, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020. For example, DOD includes hourly wages and per diem travel costs in its estimation of costs associated with a C3PAO assessment—both of which are likely to rise over time. DOD's cost estimates for a small entity's Level 3 C3PAO assessment envision one senior and three junior assessors, each of whom would spend 57 hours to conduct the assessment, for a total cost of approximately $29,000. This estimate includes five days of travel-related per diem expenses for each employee to facilitate on-site visits and assessments (estimated at $250 per day per employee); however, this estimate may not include airfare or other transportation-related expenses, which would likely significantly increase the associated costs in some instances.

Particular focus has been placed on the lack of standardized guidance to prevent "actual or potential conflicts of interest" on the part of [CMMC-AB] Board members[74] and the creation of "two layers of non-government entities [the CMMC-AB and C3PAO] … that have enormous power" to determine if a particular entity can be awarded a DOD contract.[75]

- Industry stakeholders have expressed concern regarding the interim rule's requirement for contractors to post CMMC assessment results in the Supplier Performance Risk System (SPRS) tool, contending that DOD has provided insufficient documentation that "these results [will be] safely stored and handled" via appropriate internal controls and protections.[76] SPRS could ultimately contain detailed documentation regarding virtually every DIB entity's cybersecurity "operational practices and security posture," making the system an attractive target for "malign actors" unless adequately secured.[77]
- Some in industry view the CMMC framework, when assessed as a whole together with additional contractual requirements and restrictions introduced in recent years such as those introduced by Section 889(a)(1)(B) of the FY2019 NDAA (P.L. 115-232) and the ongoing economic impact of the COVID-19 pandemic, as an entry barrier to the defense acquisition system that will further dissuade small businesses and nontraditional defense contractors from engaging with the DOD.[78]

# Issues for Congress

Some analysts have described prior congressional and DOD efforts to mitigate cybersecurity risks and vulnerabilities as fragmentary and reactive to specific issues or emerging concerns, with the potential to create "confusion" within the defense industrial base as contractors attempt to meet "ever-changing" requirements seen by some within the industry as costly and overly burdensome.[79] Other observers have also argued that the current system, which largely turns on self-reporting cybersecurity breaches and losses of certain types of federal information, has "demonstrably failed," in part due to "a scarcity of resources" and difficulties involved in

[74] Letter to the Office of the Under Secretary of Defense for Acquisition & Sustainment from the National Defense Industrial Association, "Re: Industry Questions on CMMC Implementation," October 8, 2020.

[75] Frank Kendall, "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May," *Forbes*, April 29, 2020.

[76] Information Technology Industry Council (ITI), letter to the Department of Defense, "RE: DFARS Case 2019-D041," November 30, 2020, p. 8.

[77] Information Technology Industry Council (ITI), letter to the Department of Defense, "RE: DFARS Case 2019-D041," November 30, 2020, p. 8.

[78] Frank Kendall, "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May," *Forbes*, April 29, 2020.

[79] U.S. Congress, Senate Committee on Armed Services, Subcommittee on Cybersecurity, *Cybersecurity Responsibilities of the Defense Industrial Base*, 116th Cong., 1st sess., March 26, 2019 and Ian Brekke, "DOD Continues to Up the Ante on Cybersecurity Compliance for Contractors," *Inside Government Contracts*, January 29, 2019, available at https://www.insidegovernmentcontracts.com/2019/01/dod-continues-ante-cybersecurity-compliance-contractors/. Also see, for example, Council of Defense and Space Industry Associations, *Re: DFARS Case 2013-D018; Network Penetration Reporting and Contracting for Cloud Services*, November 17, 2017. See also CRS Report R45491, *Science and Technology Issues in the 116th Congress*, coordinated by Frank Gottron.

tracking breaches at contractors and subcontractors.[80] These experts focus on the limited mechanisms available to the legislative and executive branches to influence the behaviors of private-sector organizations, seeing DOD's implementation of the CMMC framework as a reasonable, necessary initiative that responds to "pervasive and persistent vulnerabilities to the industrial base" by creating a baseline requirement for security in the performance of government contract work.[81]

While acknowledging the need for improved cybersecurity within the DIB sector, others question some aspects of the implementation of the CMMC framework. Particular focus has been placed on the role and influence of the CMMC-AB;[82] the potential for CMMC requirements to increase DOD costs and slow the acquisition process; the degree to which the CMMC framework requirements could dissuade nontraditional contractors and small businesses from seeking government work;[83] and outstanding questions related to the specifics of the CMMC certification process, such as how disputed assessments would be addressed and resolved.[84]

[80] Gordon Lubold and Dustin Volz, "Navy, Industry Partners Are 'Under Cyber Siege' by Chinese Hackers, Review Asserts," *The Wall Street Journal*, March 12, 2019.

[81] Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States*, September 2018, p. 88.

[82] See, for example, Frank Kendall, "Cybersecurity Maturity Model Certification: An Idea Whose Time Has Not Come and Never May," *Forbes*, April 29, 2020, available at https://www.forbes.com/sites/frankkendall/2020/04/29/cyber-security-maturity-model-certificationan-idea-whose-time-has-not-come-and-never-may/#3282ff033bf2.

[83] See for example Department of Defense, "Under Secretary of Defense for Acquisition & Sustainment (USD(A&S) Ellen Lord Press Briefing on Defense Acquisition," transcript, December 10, 2019, available at https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2037206/under-secretary-of-defense-for-acquisition-sustainment-ellen-lord-press-briefin/ (see exchange between Anthony Capaccio, Bloomberg and USD(A&S) Lord); see also Tony Bertuca, "Dominance of 'nontraditional' players in DOD's prototype pipeline raises questions about next-gen weapons," *Inside Defense*, October 23, 2020, available at https://insidedefense.com/daily-news/dominance-nontraditional-players-dods-prototype-pipeline-raises-questions-about-next-gen.

[84] See, for example, letter to the Office of the Under Secretary of Defense for Acquisition & Sustainment from the National Defense Industrial Association, "Re: Industry Questions on CMMC Implementation," October 8, 2020, available at https://www.ndia.org/-/media/sites/ndia/policy/blog/documents/cmmc-outstanding-questions-fall-2020.ashx?la=en.

# Appendix A. Current Regulatory and Statutory Treatment of Cybersecurity Risk and Vulnerability Mitigation in the Defense Industrial Base

## Selected Statutory Requirements

### Information Sharing, Notification, and Reporting Requirements

The following discussion focuses on *DOD-specific* statutory information sharing and notification requirements. Other authorities and responsibilities with respect to cybersecurity information sharing and notification requirements across the federal government are established primarily under Title 6 (6 U.S.C. §§1501-1510) of the U.S. Code.[85]

### Reporting of Cyber Incidents Experienced by Operationally Critical Contractors

As enacted by Section 1632 of the Fiscal Year (FY) 2015 National Defense Authorization Act (NDAA, P.L. 113-291), 10 U.S.C. §391 requires the Secretary of Defense to establish procedures for mandatory reporting to a designated DOD component each time a cyber incident affects the network or information systems of operationally critical contractors, as designated by the Secretary of Defense.

A *cyber incident* is defined as "actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein." *Operationally critical contractor* is defined as a contractor designated by the Secretary of Defense "as a critical source of supply for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation."

Such reports must include the contractor's assessment of the effect of the cyber incident on the ability of the contractor to meet its contractual requirements. Any such reporting procedures developed by the department also must include mechanisms for DOD personnel to provide assistance in detecting and mitigating penetrations, and establish that such access to a contractor's equipment or information is limited to determining whether, and what, DOD-related information was successfully exfiltrated (or stolen) from a network or information system of a contractor.

The provision was enacted in part due to the findings of a 2014 Senate Armed Services Committee investigation into cyber intrusions affecting U.S. Transportation Command (TRANSCOM) contractors.[86] The committee's investigation "identified approximately 50 successful intrusions or other cyber events … targeting TRANSCOM contractors between June 1,

[85] For an overview of additional related congressional and executive branch actions, see CRS Report R43317, *Cybersecurity: Legislation and Hearings, 115th-116th Congresses*, by Rita Tehan and CRS Report R44427, *Cybersecurity: Federal Government Authoritative Reports and Resources*, by Rita Tehan.

[86] U.S. Senate Committee on Armed Services, "SASC Investigation Finds Chinese Intrusions into Key Defense Contractors," press release, September 17, 2014, available at https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors.

2012 and May 30, 2013," many of which the committee's investigators attributed to individuals associated with the Chinese government.[87]

In the Senate report language for the FY2015 NDAA, the Senate emphasized the need for DOD awareness of "successful cyber intrusions … into the computer networks of operationally critical contractors so that TRANSCOM and other potentially affected combatant commands can assess the risks to contingency operations posed by those intrusions and adjust operational plans, if necessary."[88]

## Reporting of Penetration of Covered Networks or Information Systems Operated by Cleared Defense Contractors

As originally enacted by Section 941 of the FY2013 NDAA (P.L. 112-239), 10 U.S.C. §393 requires the Secretary of Defense to establish procedures for mandatory reporting to a designated DOD component when certain types of covered networks or information systems operated by cleared defense contractors are successfully penetrated.[89]

This provision defines a *cleared defense contractor* as a "private entity granted clearance by the [DOD] to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the [DOD]." *Covered network* is defined as "a network or information system of a cleared defense contractor that contains or processes information created by or for the [DOD] with respect to which such contractor is required to apply enhanced protection." The term *penetrated* is not defined.

Such reports are required to include, among other components, a description of the technique or method used in penetrating covered networks or information systems; a sample of the malicious software—if discovered and isolated by the contractor—involved in the penetration; and a summary of information created by or for the DOD in connection with any DOD program that has been potentially compromised.

The established reporting procedures also must include mechanisms for DOD personnel to obtain—upon request—access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis in addition to any analysis conducted by the defense contractor. Such procedures must establish that such access to a contractor's equipment or information is limited to determining whether information created by or for the DOD in connection with any DOD program was successfully exfiltrated from a network or information system of the contractor and, if so, what information was exfiltrated. These mechanisms must also provide for reasonable protection of trade secrets; commercial or financial information; and information that can be used to identify a specific person.

### *Defense Industrial Base Cybersecurity Program*

In part to implement the requirements of 10 U.S.C. §391 and 10 U.S.C §393, the DOD established the Defense Industrial Base (DIB) Cybersecurity (CS) Program to "enhance and

[87] U.S. Congress, Senate Committee on Armed Services, *Inquiry Into Cyber Intrusions Affecting U.S. Transportation Command Contractors*, 113th Cong., 2nd sess., September 18, 2014, S.Rept. 113-258.

[88] U.S. Congress, Senate Committee on Armed Services, *Carl Levin National Defense Authorization Act for Fiscal Year 2015*, report to accompany S. 2410, 113th Cong., 2nd sess., June 2, 2014, S.Rept. 113-176, pp. 228-229.

[89] The provision was originally set out as a note under 10 U.S.C. §2224 before being transferred and renumbered as 10 U.S.C. §393 by Section 1641 of P.L. 114-92, the FY2016 NDAA.

supplement DIB participants' capabilities to safeguard … information that resides on or transits DIB unclassified networks or information systems."[90]

Under the DIB CS Program, DOD and DIB participants share unclassified and classified cyber threat information. In addition to the statutory reporting requirements, DOD permits eligible defense contractors to voluntarily participate in the DIB CS program to share cyber threat information and cybersecurity best practices with other DIB CS participants.

## Congressional Notification of Cybersecurity Breaches and Loss of Personally Identifiable Information and Controlled Unclassified Information

Section 1639 of the FY2019 NDAA (10 U.S.C. §2224 note) requires the Secretary of Defense to notify the defense committees in writing when there is an occurrence of a significant loss of personally identifiable information of civilian or uniformed members of the Armed Forces, or a significant loss of controlled unclassified information by a cleared defense contractor.

This provision defines *significant loss of controlled unclassified information* as "an intentional, accidental, or otherwise known theft, loss, or disclosure of [DOD] programmatic or technical controlled unclassified information the loss of which would have significant impact or consequence to a program or mission of the [DOD], or the loss of which is of substantial volume." *Significant loss of personally identifiable information* is defined as "an intentional, accidental, or otherwise known disclosure of information that can be used to distinguish or trace an individual's identity [such as demographic, personnel, medical, or financial information] involving 250 or more civilian or uniformed members of the Armed Forces."

The Secretary of Defense is further required to establish procedures for the protection of operational integrity, personally identifiable information of civilian and uniformed members of the Armed Forces, and controlled unclassified information.

In the FY2019 NDAA conference report, Congress expressed its concern over reports regarding the theft of a significant quantity of data relating to submarines and underwater weaponry from a contractor working with the U.S. Navy's Naval Undersea Warfare Center:

> [Also] troubling … the congressional defense committees were only alerted to this significant breach months after the initial loss. While the conferees understand that extenuating circumstances dictated that senior members of Navy leadership were similarly late to notification of the theft and that the investigation is on-going, this communication delay, both within the [DOD] and across the branches of government, is unacceptable for a loss of this magnitude.
>
> The conferees thus expect the congressional defense committees to be notified … of future losses of controlled information and will continue to exercise their oversight and legislative responsibilities to correct the failures evinced in this incident.[91]

[90] Office of the DOD Chief Information Officer, "Department of Defense (DoD)-Defense Industrial Base (DIB) Cybersecurity (CS) Activities," 80 *Federal Register* 59581, October 2, 2015 and 32 C.F.R. Part 236; see also DIB Cyber Incident Reporting & Cyber Threat Information Sharing Portal, "About the DIB CS Program," available at https://dibnet.dod.mil/portal/intranet/Splashpage/RegisterThemed.

[91] U.S. Congress, House Committee on Armed Services, *John S. McCain National Defense Authorization Act for Fiscal Year 2019*, conference report to accompany H.R. 5515, 115th Cong., 2nd sess., July 23, 2018, H.Rept. 115-863, pp. 1053-1054. See also Ellen Nakashima and Paul Sonne, "China Hacked a Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare," *The Washington Post*, June 8, 2018, available at 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.

# Regulatory Requirements

The following discussion focuses on currently implemented regulatory requirements.

## Federal Acquisition Regulation Changes

### *Safeguarding Contractor Information Systems*

In 2016, the Federal Acquisition Regulation (FAR) was amended to add a new subpart and contract clauses establishing policies for the basic safeguarding of contractor information systems that process, store or transmit federal contract information.[92] A brief summary of each added subpart and contract clause follows:

- ***FAR Subpart 4.19*** establishes the applicability of requirements for basic safeguarding of covered contractor information systems, stating that the subpart applies to all acquisitions, including commercial items other than commercially available off-the-shelf items when a contractor's information system may contain federal contract information; and requires the insertion of a prescribed clause (FAR subpart 52.204-21) in solicitations and contracts when the contractor or a subcontractor at any tier may have federal contract information residing in or transiting through its information system;
- ***FAR Subpart 7.015(b)(18)*** requires the consideration of security of federal contract information during the acquisition planning process;
- ***FAR Subpart 12.301(d)(3)*** requires the insertion of a prescribed clause (FAR contract clause 52.204-21) in solicitations and contracts for the acquisition of commercial items, except commercially available off-the-shelf items; and
- ***FAR Contract Clause 52.204-21*** establishes minimum requirements and procedures for the basic safeguarding of covered contractor systems, to include security controls such as limiting system access to authorized users; authenticating the identities of system users; limiting physical access to systems and related infrastructure to authorized individuals; protecting systems from malicious code; and identifying and correcting system flaws in a timely manner.

These policies and clauses do not absolve contractors from compliance with any other specific safeguarding requirements and procedures specified by federal agencies and departments relating to covered contractor information systems generally or other federal requirements for safeguarding controlled unclassified information as established by Executive Order 13556.

## Defense Federal Acquisition Regulation Supplement Changes

### *Safeguarding Unclassified Controlled Technical Information and Cyber Intrusion Reporting Requirements*

In 2013, the DOD issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to add a new subpart and contract clauses requiring the implementation of adequate security measures to safeguard unclassified DOD controlled technical information

[92] DOD, GSA, and NASA, "Federal Acquisition Regulation; Basic Safeguarding of Contractor Information Systems," 81 *Federal Register* 30439, May 16, 2016.

within contractor information systems from unauthorized access and disclosure, and to mandate the reporting of certain cyber intrusion events that affect DOD information resident on or transiting through contractor unclassified information systems.[93] The DFARS defines *adequate security* as protective measures equivalent to the consequences and probability of loss, misuse, or unauthorized access to, or modification of information. A brief summary of each added subpart and contract clause as currently implemented—barring those associated with CMMC discussed earlier in this report—follows:

- ***DFARS Subpart 204.73*** establishes related definitions, policy, procedures, and requires the insertion of prescribed clauses in all solicitations and contracts, including solicitations and contracts using FAR Part 12 procedures for the acquisition of commercial items. DFARS Subpart 204.73 states that it is DOD policy that the department, its contractors, and its subcontractors will provide adequate security to safeguard unclassified controlled technical information on unclassified information systems from unauthorized access and disclosure. It requires contractors to report to the DOD certain cyber incidents within 72 hours of discovery that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems;[94]
- ***DFARS Subpart 212.301*** requires the insertion of a prescribed clause in solicitations and contracts for the acquisition of commercial items;[95]
- ***DFARS Solicitation Provision 252.204-7008*** is required to be included in all solicitations (including solicitations using FAR Part 12 procedures, except for solicitations solely for the acquisition of commercially available off-the-shelf items);[96]
- ***DFARS Contract Clause 252.204-7009*** establishes limitations on the use or disclosure of third-party contractor reported cyber incident information by a contractor and is required in all solicitations and contracts, including solicitations and contracts using FAR Part 12 for services that include support for the DOD's activities related to safeguarding covered defense information and cyber incident reporting;[97]
- ***DFARS Contract Clause 252.204–7012*** is required in all contracts and solicitations (including those using FAR Part 12 procedures, except for contracts and solicitations solely for the acquisition of commercially available off-the-shelf items), and must be also included in subcontracts for which performance will involve covered defense information or operationally critical support. The clause requires contractors and subcontractors to:

[93] DOD, "Defense Federal Acquisition Regulation Supplement: Safeguarding Unclassified Controlled Technical Information (DFARS Case 2011-D039)," 78 *Federal Register* 69273, November 18, 2013.

[94] DFARS, Subpart 204.73, "Safeguarding Covered Defense Information and Cyber Incident Reporting," available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm.

[95] DFARS, Subpart 212.3, "Solicitation Provisions and Contract Clauses for the Acquisition of Commercial Items," available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/212_3.htm.

[96] DFARS, Part 252 - Solicitation Provisions and Contract Clauses, Subsection 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls," available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7008.

[97] DFARS, Part 252 - Solicitation Provisions and Contract Clauses, Subsection 252.204-7009, "Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information," available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7009.

(1) safeguard covered defense information by, at a minimum, implementing the requirements of NIST Special Publication 800-171 as soon as practicable but not later than December 31, 2017;

(2) report cyber incidents that affect covered defense information, or that affect the contractor's ability to perform requirements designated as operationally critical support;

(3) submit malicious software discovered and isolated in connection with a reported cyber incident to the DOD Cyber Crime Center; and

(4) facilitate damage assessments in the event of a cyber incident by providing media and damage assessment information upon request.[98]

[98] DFARS, Part 252 - Solicitation Provisions and Contract Clauses, Subsection 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," available at https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

# Appendix B. NIST Special Publication 800-171

NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," details recommended security requirements, grouped into fourteen *families*, for protecting controlled unclassified information (CUI) in components of nonfederal systems that process, transmit, or store CUI, or that provide security protection for such components.[99] Each requirement family includes *basic security requirements* framed as overarching responsibilities (e.g., limiting system access to authorized users) and *derived security requirements* framed as specific tasks required to carry out an overarching responsibility (e.g., using multifactor authentication to limit system access).[100]

Contractors are required to self-certify through the submission of a *system security plan* that details how the specified security requirements under each family have been met – or provides the contractor's plans to meet the requirements – and must further develop "plans of action that describe how any unimplemented security requirements will be met and how any planned mitigations will be implemented."[101] The DOD issued guidance in November 2018 for assessing contractors' system security plans and their implementation of the security controls required by NIST Special Publication 800-171, as required by DFARS clause 252.204–7012.[102]

The DOD has developed a standard assessment methodology to evaluate contractor implementation of the NIST SP 800-171 requirements.[103]

[99] National Institute of Standards and Technology (NIST),, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171, Revision 2, updated as of February 21, 2020, available at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[100] NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171, Revision 2, updated as of February 21, 2020, available at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final. Other related NIST publications include NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations* (which provides additional details regarding the required security and privacy controls), and NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (see especially Sections 3.3 to 3.6, which provides a systematic process for identifying, implementing, assessing and monitoring the controls), provide additional related information.

[101] NIST, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171, Revision 2, updated as of February 21, 2020, available at https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final.

[102] Office of the Under Secretary of Defense (Acquisition and Sustainment), "Guidance for Assessing Compliance and Enhancing Protections Required by DFARS Clause 252.204–7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," memorandum, November 6, 2018 available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/Guidance_for_Assessing_Compliance_and_Enhancing_Protections.pdf . See also additional DOD policy guidance available at https://www.acq.osd.mil/dpap/pdi/cyber/guidance_for_assessing_compliance_and_enhancing_protections.html.

[103] DARS, Department of Defense, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," 85 *Federal Register* 61505-61522, September 29, 2020. See also NIST SP 800-171 DOD Assessment Methodology, Version 1.2.1, June 24, 2020, available at https://www.acq.osd.mil/dpap/pdi/cyber/docs/NIST%20SP%20800-171%20Assessment%20Methodology%20Version%201.2.1%20%206.24.2020.pdf.

# Appendix C. Overview of CMMC Domains and Capabilities

**Table C-1. CMMC Framework, by Domains and Capabilities**

| Domain | Capability |
|---|---|
| • Access Control | • Establish system access requirements<br>• Control internal system access<br>• Control remote system access<br>• Limit data access to authorized users and processes |
| • Asset Management | • Identify and document assets<br>• Manage asset inventory |
| • Audit and Accountability | • Define audit requirements<br>• Perform auditing<br>• Identify and protect audit information<br>• Review and manage audit logs |
| • Awareness and Training | • Conduct security awareness activities<br>• Conduct training |
| • Configuration Management | • Establish configuration baselines<br>• Perform configuration and change management |
| • Identification and Authentication | • Grant access to authenticated entities |
| • Incident Response | • Plan incident response<br>• Detect and report events<br>• Develop and implement a response to a declared incident<br>• Perform post incident reviews<br>• Test incident response |
| • Maintenance | • Manage maintenance |
| • Media Protection | • Identify and mark media<br>• Protect and control media<br>• Sanitize media<br>• Protect media during transport |
| • Personnel Security | • Screen personnel<br>• Protect CUI during personnel actions |
| • Physical Protection | • Limit physical access |
| • Recovery | • Manage backups<br>• Manage information security continuity |
| • Risk Management | • Identify and evaluate risk<br>• Manage risk<br>• Manage supply chain risk |

| | |
|---|---|
| • Security Assessment | • Develop and manage a system security plan<br>• Define and manage controls<br>• Perform code reviews |
| • Situational Awareness | • Implement threat monitoring |
| • Systems and Communications Protection | • Define security requirements for systems and communications<br>• Control communications at system boundaries |
| • System and Information Integrity | • Identify and manage information system flaws<br>• Identify malicious content<br>• Perform network and system monitoring<br>• Implement advanced email protections |

**Source:** Office of the Under Secretary of Defense for Acquisition and Sustainment, "Cybersecurity Maturity Model Certification," version 1.02, March 18, 2020, p. 8, available at https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf.

## Author Information

Heidi M. Peters
Analyst in U.S. Defense Acquisition Policy

## Acknowledgments

The author is grateful to Research Assistant Hibbah Kaileh and Visual Information Specialist Jamie Hutchinson for assistance in preparing this report.

## Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.