United States Government Accountability Office

Report to Congressional Committees

December 2021

DEFENSE CONTRACTOR CYBERSECURITY

Stakeholder Communication and Performance Goals Could Improve Certification Framework

Accessible Version

GAO@100
A Century of Non-Partisan Fact-Based Work

GAO-22-104679

GAO Highlight

Highlights of GAO-22-104679, a report to congressional committees

December 2021

DEFENSE CONTRACTOR CYBERSECURITY

Stakeholder Communication and Performance Goals Could Improve Certification Framework

Why GAO Did This Study

DOD relies on thousands of defense contractors for goods and services ranging from weapon systems to analysis to maintenance. In doing business with DOD, these companies access and use sensitive unclassified data. Accordingly, the department has taken steps intended to improve the cybersecurity of this defense industrial base.

A Senate report included a provision for GAO to review DOD's implementation of CMMC. This report addresses (1) what steps DOD took to develop CMMC, (2) the extent to which DOD made progress in implementing CMMC, including communication with industry, and (3) the extent to which DOD has developed plans to assess the effectiveness of CMMC.

GAO reviewed DOD documents related to the design and implementation of CMMC and interviewed DOD officials involved in designing and managing it. GAO also interviewed representatives from defense contractors, industry trade groups, and research centers.

What GAO Recommends

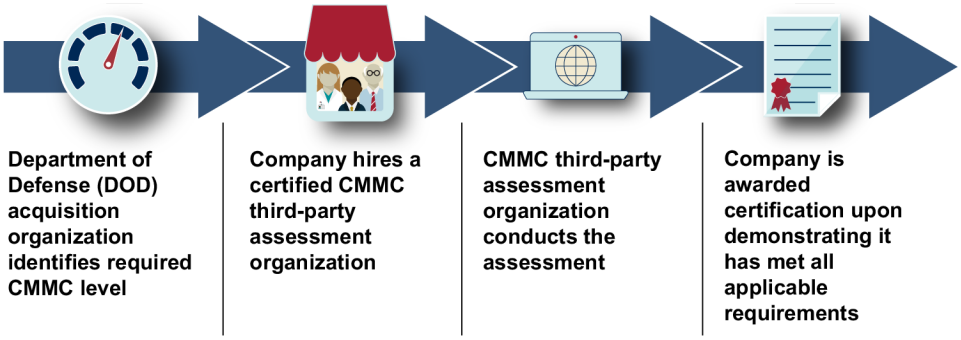
GAO is making three recommendations to DOD to improve communication to industry, develop a plan to evaluate the pilot, and develop outcome-oriented performance measures. DOD concurred with the recommendations and outlined plans to address them in CMMC 2.0.

View GAO-22-104679. For more information, contact W. William Russell at (202) 512-4841 or russellw@gao.gov, Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov, or Jennifer R. Franks at (404) 679-1381 or franksj@gao.gov.

What GAO Found

For years, malicious cyber actors have targeted defense contractors to access sensitive unclassified data. In response, since 2019, the Department of Defense (DOD) has engaged with a range of stakeholders to develop and refine a set of cybersecurity practices and processes for contractors to use to help assure security of the data. For relevant contracts, this Cybersecurity Maturity Model Certification (CMMC) requires that defense contractors implement these practices and processes on their information systems and networks.

Key Steps in CMMC Verification Process



Source: GAO summary of DOD's Cybersecurity Maturity Model Certification (CMMC) implementation activities. | GAO-22-104679

DOD began CMMC implementation with an interim rule that took effect in November 2020, but the rollout of the 5-year pilot phase is delayed. For example, DOD planned to pilot the CMMC requirement on up to 15 acquisitions in fiscal year 2021 but has not yet included the requirement in any acquisitions, in part due to delays in certifying assessors. Industry—in particular, small businesses—has expressed a range of concerns about CMMC implementation, such as costs and assessment consistency. DOD engaged with industry in refining early versions of CMMC, but it has not provided sufficient details and timely communication on implementation. Until DOD improves this communication, industry will be challenged to implement protections for DOD's sensitive data.

DOD has identified plans to assess aspects of its CMMC pilot, including high-level objectives and data collection activities, but these plans do not fully reflect GAO's leading practices for effective pilot design. For example, DOD has not defined when and how it will analyze its data to measure performance. Further, GAO found that DOD has not developed outcome-oriented measures, such as reduced risk to sensitive information, to gauge the effectiveness of CMMC. Without such measures, the department will be hindered in evaluating the extent to which CMMC is increasing the cybersecurity of the defense industrial base.

In November 2021, DOD announced CMMC 2.0, which includes a number of significant changes, including eliminating some certification levels, DOD-specific cybersecurity practices, and assessment requirements. DOD also announced that it intended to suspend the current CMMC pilot and initiate a new rulemaking period to implement the revised framework.

Contents

Abbreviations

CMMC	Cybersecurity Maturity Model Certification
CMMC-AB	CMMC Accreditation Body
CUI	controlled unclassified information
DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	defense industrial base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DOD	Department of Defense
FAQ	frequently asked questions
FAR	Federal Acquisition Regulation
FCI	federal contract information
FedRamp	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
NDAA	National Defense Authorization Act
NDIA	National Defense Industrial Association
NIST	National Institute of Standards and Technology
POAM	Plans of Action and Milestones
SP	special publication

441 G St. N.W.
Washington, DC 20548

December 8, 2021

Congressional Committees

For many years, malicious cyber actors have targeted defense contractors' networks and systems to access sensitive Department of Defense (DOD) data. Recent cyberattacks indicate malicious actors continue to target these systems, which may contain data DOD has identified as controlled unclassified information (CUI)—unclassified information throughout the executive branch that requires safeguarding and dissemination controls in accordance with laws, regulations, and government-wide policies. Within DOD's overall CUI program, this type of information may include data related to critical technologies—such as elements of artificial intelligence and biotechnology—and information relating to the design, development, and operations of weapons and defense-critical infrastructure. As the March 2020 report of the U.S. Cyberspace Solarium Commission states, adversary cyber threats to the U.S. cause the loss of national security information and intellectual property and create the risk that U.S. military systems could be rendered ineffective or their intended uses distorted.[1]

Over the past decade, DOD has taken steps to improve the cybersecurity of the defense industrial base (DIB)—which, according to DOD estimates, consists of over 200,000 companies.[2] These steps include adding a clause to certain DOD contracts to apply certain National Institute of Standards and Technology (NIST) security requirements on certain contractor information systems to protect DOD's CUI and other sensitive data. Building on these efforts, the National Defense Authorization Act (NDAA) for Fiscal Year 2020 directed DOD to develop a framework to enhance the cybersecurity of the DIB that includes identification of unified

[1]John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1652 (2018) established the Cyberspace Solarium Commission, a federal commission made up of members of Congress and appointees, as well as officials from several agencies, to develop a consensus on a strategic approach to defending the U.S. in cyberspace against cyberattacks of significant consequences. U.S. Cyberspace Solarium Commission, *U.S. Cyberspace Solarium Commission Final Report* (Washington, D.C.: March 2020).

[2]The DIB comprises all the companies that enable research and development, as well as design, production, delivery, and maintenance of military weapon systems, components, or parts to meet U.S. military requirements.

cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements for assessing individual contractors' cybersecurity posture. Starting in 2019, DOD created the Cybersecurity Maturity Model Certification (CMMC) framework for defense contractors that includes a third-party assessment process intended to provide DOD greater assurance that contractors have developed the processes and practices needed to protect CUI and other sensitive DOD data.

The Senate report accompanying a version of the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 included a provision for us to review DOD's implementation of CMMC.[3] This report addresses (1) what steps DOD took to develop CMMC, (2) the extent to which DOD has made progress in implementing CMMC, including communication with industry, and (3) the extent to which DOD has developed plans to assess the effectiveness of CMMC.

To answer our objectives, we reviewed key documents, including DOD and other federal cybersecurity requirements and CMMC planning and guidance documents. Additionally, we interviewed DOD officials from several components, as well as representatives from research and development centers,[4] DIB companies, and DIB trade groups to get a better understanding of their perspectives on CMMC. We also conducted discussion groups with small defense contractors, large defense contractors, and CMMC assessors and consultants. We compared aspects of DOD's efforts to implement CMMC with leading practices identified in prior GAO work. Further information on our scope and methodology can be found in appendix I.

We conducted this performance audit from December 2020 to December 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[3]Senate Report 116-236 to accompany a bill on the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283.

[4]For the purposes of this report, we use the term "research and development centers" to refer to both federally funded research and development centers and university affiliated research centers that were involved in the development of CMMC.

Background

The DIB, Key to DOD's Warfighting Capability, Is under Cyber Threat

DOD relies on a large and diverse set of companies, referred to as the DIB, to deliver a wide range of contracts for goods and services that support DOD's warfighting capability. In fiscal year 2020, DOD obligated more than $420 billion on contracts for such goods and services, from computers and guided missiles to system analysis and maintenance. DOD estimates that the DIB is comprised of more than 200,000 companies, roughly three-quarters of which are small businesses. Other businesses within the DIB include some of the world's largest corporations, such as Boeing and Lockheed Martin. DIB companies act as prime contractors and subcontractors, and may have large, complex supply chains with multiple tiers of subcontractors.

DOD has reported that the DIB is the key to preserving and extending U.S. competitive military dominance.[5] The U.S. adversaries are also aware of the DIB's importance. DOD's 2018 Defense Cyber Strategy noted that while adversaries may be deterred from engaging in an armed conflict with the U.S., they are using cyberspace operations to access our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure.[6] Further, DOD has reported that small businesses within the DIB are at particular risk. DOD's 2019 Small Business Strategy states that the DIB depends on the innovation and participation of small businesses, which are targets for some adversaries that are aggressively seeking technologies and intellectual property developed within the U.S.[7]

[5]Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of Industrial Policy, *Fiscal Year 2020 Industrial Capabilities Report to Congress* (January 2021).

[6]Department of Defense, *Department of Defense Cyber Strategy (2018): Summary* (2018).

[7]Department of Defense, *Small Business Strategy* (October 2019).

Federal Laws and Guidance Address the Nation's Continuing Cybersecurity Challenges

Federal agencies, including DOD, are dependent on information technology systems and electronic data to carry out operations and to process, maintain, and report essential information. Virtually all federal operations are supported by computer systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the security of these systems and data is vital to public confidence and the nation's safety, prosperity, and well-being. In addition, many of these systems contain vast amounts of sensitive data, thus making it imperative to protect them. Recent cyber incidents at federal agencies demonstrate the damage that increasingly sophisticated threats can cause and reinforce the importance of effectively protecting federal systems, including those used by DOD and its contractors to achieve its mission.

Safeguarding federal computer systems—including those operated or maintained by contractors—has been a longstanding concern. Underscoring the importance of this issue, we have included cybersecurity on our high risk list since 1997.[8] Congress has also enacted laws and the federal government has issued regulations and guidance that include cybersecurity requirements.

- Federal Information Security Modernization Act of 2014 (FISMA). In 2014, Congress enacted FISMA, which requires federal agencies in the executive branch to develop, document, and implement a program to provide information security for the information and information systems that support the operations and assets for the agency.[9]
- NIST guidance. NIST is responsible for developing information security standards and guidelines, including minimum requirements

[8]See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, GAO-21-119SP (Washington, D.C.: Mar. 2, 2021); and *High Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

[9]The Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, §2 (44 U.S.C. 101 note), amended the Federal Information Security Management Act of 2002 (FISMA 2002).

for federal information systems. Specific examples of guidance include the following:

- NIST Special Publication 800-53 (Revision 5), which provides guidance to agencies on the selection and implementation of information security and privacy controls for systems.[10]
- NIST Special Publication 800-171 (Revision 2), which provides recommended security requirements for protecting the confidentiality of CUI that resides in nonfederal systems and organizations.[11]

- Federal Risk and Authorization Management Program (FedRAMP). In 2011, the Office of Management and Budget established FedRAMP, which is intended to provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services. Managed by the General Services Administration, the program aims to ensure that cloud computing services have adequate information security, while also eliminating duplicative efforts and reducing operational costs.
- Federal Acquisition Regulation (FAR) changes. In 2016, the FAR established a contract clause for basic safeguarding of contractor information systems that process, store, or transmit federal contract information (FCI). FCI is generally information that is not intended for public release that is provided by or generated for the government under a contract to develop or deliver a product or service to the government.[12] These requirements include safeguards such as verifying the identity of system users and limiting access to authorized users.

[10]National Institute of Standards and Technology, *Security and Privacy Controls for Information Systems and Organizations*, Special Publication 800-53, Revision 5 (Gaithersburg, MD.: September 2020).

[11]National Institute of Standards and Technology, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Special Publication 800-171, Revision 2 (Gaithersburg, Md.: February 2020).

[12]FAR clause 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*.

DOD Has Established Requirements for Contractors to Protect Its Sensitive Information

DOD has outlined various requirements for contractors over the last few years to better protect its sensitive unclassified information.[13] In an October 2016 federal register notice, DOD modified its Defense Federal Acquisition Regulation Supplement (DFARS) in a final rule to specify that a "covered contractor information system"—an unclassified information system that is owned, or operated by or for a contractor, and that processes, stores, or transmits "covered defense information"—needs to be protected in accordance with DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting.[14] "Covered defense information" includes all of the categories of information that are considered CUI that require safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.

The final rule required applicable contracts to include DFARS clause 252.204-7012, which requires unclassified information systems that are owned, or operated by or for, a contractor and that process, store, or transmit covered defense information to be subject to security requirements in NIST Special Publication 800-171. The clause was to be implemented as soon as practical, but no later than December 31, 2017, unless a request to vary from a NIST Special Publication 800-171 security requirement was submitted to the contracting officer.

In 2019, DOD established the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) within the Defense Contract Management Agency (DCMA), which was designed to ensure contractors' compliance in safeguarding information about the weapons, equipment, and systems they develop. DOD established DIBCAC as one of several related efforts to assess contractor implementation of cybersecurity requirements at the corporate level, rather than on a contract-by-contract basis. To do so,

[13]For the purposes of this report, we use the terms "sensitive information" or "sensitive unclassified information" to collectively refer to both FCI and CUI.

[14]DFARS clause 252.204-7012. The DFARS is administered by DOD and implements and supplements the FAR. The DFARS contains requirements of law, DOD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies and procedures that have a significant effect on the public. The DFARS should be read in conjunction with the primary set of rules in the FAR.

DIBCAC conducts assessments of DIB companies using NIST Special Publication 800-171 criteria.

A 2019 DOD Office of Inspector General report found that contractors were not consistently complying with the DFARS 252.204-7012 clause requirements.[15] The report also found that DOD contracting offices were not verifying that contractors' networks met those requirements.

Further, the NDAA for Fiscal Year 2020 required that the Secretary of Defense establish a framework to enhance cybersecurity for the DIB no later than February 1, 2020.[16] The framework was required to include, among other things, the identification of unified cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements to be imposed on the DIB for the purpose of assessing the cybersecurity of individual contractors. A report from the Senate Armed Services Committee highlighted the need to hold prime contractors responsible and accountable for ensuring their suppliers are implementing cybersecurity requirements to secure DOD's technology and sensitive information.

DOD Developed CMMC to Address Concerns about Contractor Protection of Sensitive Information

CMMC is a certification framework to assess DIB implementation of DOD's cybersecurity requirements. This framework is intended to provide the department with increased assurance that the DIB can adequately protect sensitive unclassified information. Depending on the sensitivity of information to be protected, DIB companies will be required to implement cybersecurity requirements at one of five levels and submit to and pass a third-party assessment in order to receive the certification at the appropriate level. DOD and a range of nongovernmental organizations administer CMMC. The department worked with industry and research

[15]Department of Defense, Inspector General, *Audit of Protection of DOD Controlled Unclassified Information on Contractor-Owned Networks and Systems*, DODIG-2019-105 (July 23, 2019).

[16]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116–92, § 1648(a).

and development centers in developing the framework and conducted simulation exercises to inform its requirements.

CMMC Development Began in 2019

DOD began developing CMMC in 2019 and issued the initial version of the CMMC standard in January 2020. CMMC is part of DOD's response to congressional direction to develop a framework to enhance cybersecurity for the DIB. It encompasses the basic safeguarding requirements for FCI and the security requirements for CUI specified in the FAR and DFARS,[17] respectively. In addition, DOD has stated that CMMC adds a certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. For any solicitation that requires a given CMMC level, a DIB company must pass the third-party assessment at that level prior to contract award.

Initial CMMC Standard Builds on Existing Cybersecurity Requirements

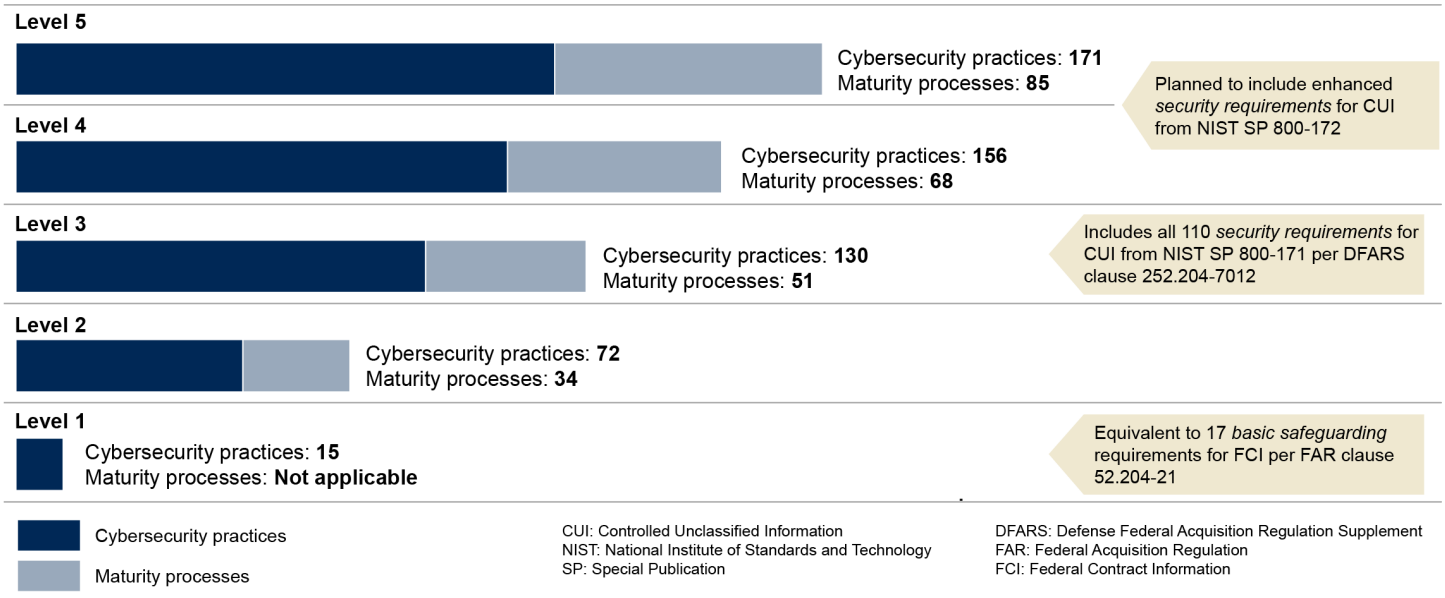
The initial CMMC standard, which DOD issued in January 2020, identifies requirements DIB companies must meet to demonstrate that they have implemented sufficient safeguards to protect DOD's sensitive unclassified information. CMMC includes two general types of cybersecurity requirements: practices and processes. Practices are activities performed to implement cybersecurity, ranging from "basic cyber hygiene" at the lowest level to "highly advanced cybersecurity" at the highest level. Processes characterize the extent to which an organization has institutionalized cybersecurity practices, ranging from "performed" at the lowest level to "optimized" at the highest level.

Recognizing that not all unclassified data require the same degree of protection, CMMC is organized into five levels. The practices and processes in each level are intended to reflect the type and sensitivity of the information that must be protected against anticipated threats. The DOD organization responsible for the acquisition must determine the appropriate CMMC certification level requirement based on the sensitivity of the acquisition's underlying data. For example, CMMC level 1 includes

[17]FAR clause 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*; DFARS clause 252.204-7012.

17 practices associated with basic cybersecurity safeguards for protecting less sensitive data, such as FCI, but does not include any processes to demonstrate that an organization has institutionalized those practices. Comparatively, CMMC level 3 includes 130 practices, including all 110 security controls in NIST Special Publication 800-171. Further, this level includes 51 processes to ensure an organization has established, maintained, and identified resources to implement a plan for institutionalizing those practices, among other things.[18] Figure 1 shows the number of practices and processes included at each level of CMMC in the initial standard.

Figure 1: Number of Practices and Processes, by Level, in the Initial Cybersecurity Maturity Model Certification Standard, as of October 2021



Source: GAO analysis of Department of Defense's Cybersecurity Maturity Model Certification (CMMC) requirements. | GAO-22-104679

Note: Information in this figure is current as of October 2021. In November 2021, DOD released CMMC 2.0, which includes a number of significant modifications to the initial framework and standard.

According to DOD officials, CMMC levels 4 and 5, which have not yet been finalized, will include additional practices and processes intended to protect against the most sophisticated types of cyber threats, such as

[18]There are three maturity processes associated with CMMC level 3. Each process applies to 17 different areas so companies must demonstrate they have implemented 51 process-related requirements to achieve CMMC level 3.

security controls from NIST Special Publication 800-172.[19] Program officials also said they do not expect DOD will use CMMC level 2 as a contract requirement. Rather, it is intended as interim step for DIB companies that are seeking to progress from level 1 to level 3.

CMMC Includes a Verification Process

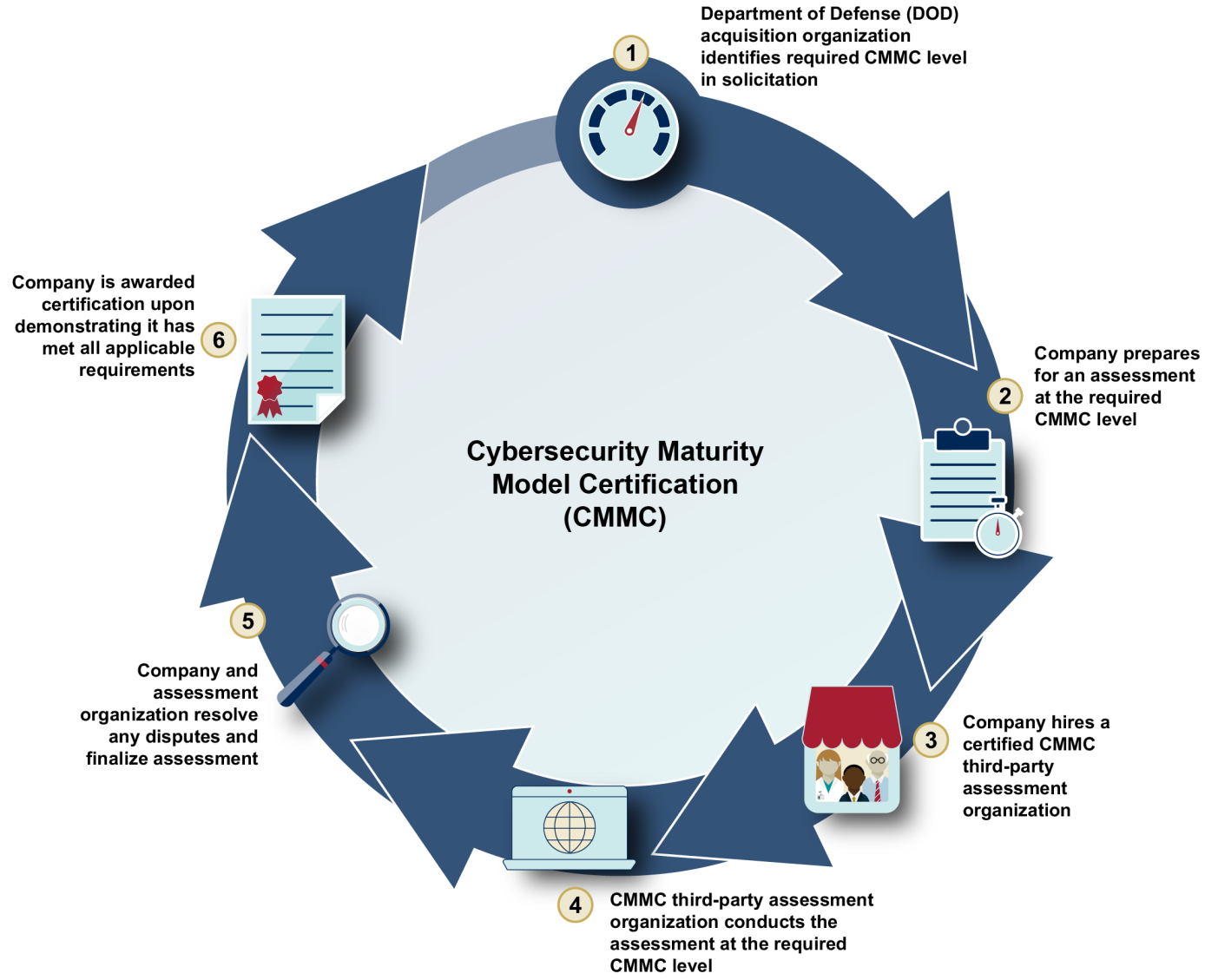
In addition to the initial CMMC standard, DOD has also defined some key portions of the CMMC verification process. The verification process is the method by which a third-party assessment organization determines whether a DIB company has achieved one of the five certification levels. In November 2020, DOD issued two CMMC assessment guides, one for level 1 and another for level 3. The assessment guides outline how the third-party organizations should conduct their assessments, including the criteria by which the assessors will evaluate each practice and process. For a CMMC level 3 assessment, for example, a DIB company must provide evidence that it has implemented all 130 practices and 51 processes.

According to the CMMC framework, after identifying a target DOD solicitation and the associated CMMC level requirement as specified by the acquisition organization, a DIB company is to conduct a self-assessment and then hire a certified CMMC third-party assessment organization to conduct the assessment. The assessment organization is then to review the evidence, interview DIB company personnel, or conduct tests—or some combination thereof—to determine the score (met, not met, or not applicable) for each practice and process. If all requirements are scored as met or not applicable, the CMMC assessment organization issues the DIB company a certification at the level required in the solicitation. If any of the requirements are scored as not met, the DIB company cannot receive certification at the required level. After being certified and awarded a contract, a DIB company must maintain a current (not older than 3 years) CMMC certification at the level required in the contract for the duration of the contract and will be required to renew its

[19]National Institute of Standards and Technology, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, Special Publication 800-172 (Gaithersburg, Md.: February 2021). This publication provides federal agencies with recommended enhanced security requirements for protecting the confidentiality of CUI when the information is resident in nonfederal systems, among other things.

certification every 3 years to continue to receive DOD awards. Figure 2 shows the major steps involved in obtaining a CMMC certification.

Figure 2: CMMC Verification Process, as of October 2021



Source: GAO analysis of DOD's CMMC certification process. | GAO-22-104679

Note: Information in this figure is current as of October 2021. In November 2021, DOD released CMMC 2.0, which includes a number of significant modifications to the initial framework and standard.

DOD and Nongovernment Organizations Have Roles Administering CMMC

A range of organizations, which DOD collectively refers to as the CMMC ecosystem,[20] have an important role in supporting or executing CMMC. The CMMC ecosystem includes several DOD organizations as well as nongovernment organizations that perform key tasks within CMMC, including the assessments. Conducting CMMC assessments for the entire DIB will require thousands of assessors as well as infrastructure to train, accredit, and provide oversight of the assessment community. Table 1 lists key organizations within the CMMC ecosystem and some of their roles.

Table 1: The Cybersecurity Maturity Model Certification Ecosystem

Organization	Type of Organization	Key Roles
Program Office, Industrial Policy, Office of the Under Secretary of Defense for Acquisition and Sustainment	DOD	• Provides oversight. • Develops and publishes policies and requirements. • Coordinates rulemaking activities. • Manages pilot acquisitions. • Establishes assessment and training requirements.
Accreditation Body	Nongovernment	• Authorizes and accredits assessment organizations. • Facilitates information sharing through town halls. • Maintains a list of authorized and accredited assessment organizations on a public website called the Marketplace.
Assessors and Instructors Certification Organization	Nongovernment	• Certifies assessors and instructors. • Defines training objectives, designs curricula, and develops training materials for assessors and instructors.
Defense Contract Management Agency, Defense Industrial Base Cybersecurity Assessment Center	DOD	• Conducts assessments on candidate third-party assessment organizations before they are certified as assessment organizations.
Certified Third-Party Assessment Organizations	Nongovernment	• Conducts assessments to verify that a defense contractor has satisfied the cybersecurity requirements at a specific certification level required by the solicitation and defense contract. • Issues decisions on assessment appeals if an assessed company chooses to appeal the results of an assessment based on perceived errors or other factors.

[20]DOD's use of the term "ecosystem" is similar to NIST's definition of a "data processing ecosystem," which is the complex and interconnected relationships among entities involved in creating or deploying systems, products, or services or any components that process data.

Source: GAO analysis of Department of Defense (DOD) Information. | GAO-22-104679.

Note: Information in this table is current as of October 2021. In November 2021, DOD released CMMC 2.0, which includes a number of significant modifications to the initial framework and standard.

The CMMC program office has the primary responsibility within DOD for managing and overseeing CMMC. In addition to developing CMMC standards, guides, and policies for implementation, the program office establishes requirements for the other members of the CMMC ecosystem. For example, DOD is responsible for establishing CMMC assessment and training requirements, as well as developing the CMMC assessment guides that identify the criteria assessors must use when conducting assessments.

DOD chose to partner with nongovernment entities in executing CMMC to address the challenge of conducting assessments for the entire DIB. According to DOD's analysis, given the size and scale of the DIB, the department cannot attain sufficient government cybersecurity assessment capability to conduct the thousands of assessments it estimated will be needed every year to support CMMC. As a result, in March 2020, the department signed a memorandum of understanding with the CMMC Accreditation Body (CMMC-AB), a non-profit corporation founded in January 2020 that authorizes and accredits the third-party organizations that will conduct assessments. In November 2020, DOD awarded the CMMC-AB a no-cost contract, solidifying the CMMC-AB's responsibilities. According to the contract, the CMMC-AB must report to DOD its plans for raising revenue, which may include fees, licensing, membership, and partnerships. The CMMC-AB communicates relevant training information through its website and other means, including periodic town hall events.

The CMMC-AB is working to create a separate entity—the CMMC Assessors and Instructors Certification Organization—to develop and administer training and testing materials for individual members of the CMMC ecosystem.[21] Both assessment organizations and individual assessors must be approved by the CMMC-AB and the CMMC Assessors and Instructors Certification Organization, respectively, to conduct CMMC assessments.

[21]The CMMC-AB is authorizing and accrediting the separate Assessors and Instructors Certification Organization in accordance with the contract signed with DOD. The contract also requires the CMMC-AB to achieve compliance with international standards for accreditation bodies.

DIBCAC—within DCMA—is another DOD organization that has an important role in administering aspects of CMMC. DIBCAC conducts assessments of approved CMMC third-party assessment organizations as part of the final step in their certification. These third-party organizations must pass a DIBCAC assessment and receive CMMC certification before they can be authorized to conduct CMMC assessments.

Third-party assessment organizations will be responsible for verifying the implementation of processes and practices associated with the achievement of a given CMMC level. These organizations are to employ CMMC assessors who have been certified by the CMMC-AB and trained through the CMMC Assessors and Instructors Certification Organization. DIB companies are then to hire a third-party assessment organization to conduct their assessment. If the DIB company has met all applicable requirements, the assessment organization will issue the DIB company a CMMC certification.

DOD Initially Engaged with Stakeholders to Refine CMMC and Conduct Simulation Exercises

DOD engaged with a range of stakeholders, including DIB trade groups and research and development centers, to develop and refine the framework prior to issuing the initial CMMC standard in the January 2020 version 1.0 of CMMC. Between September and December 2019, DOD released three versions of the CMMC model for public review and feedback and, according to program officials, received over 2,500 comments.

During group discussions with large defense contractors, participants said that DOD was particularly responsive to feedback in reducing the number of practices from the earliest drafts of CMMC to the initial standard DOD released in January 2020. For example, in official comments to the CMMC program office from September 2019, the U.S. Small Business Administration's Office of Advocacy stated that small businesses may have problems with the complexity of implementing CMMC and that they hoped the program office would aggressively pare down the number of requirements. CMMC program officials said that they significantly reduced the size and complexity of the CMMC standard in response to comments from the Small Business Administration, the public, and other DOD stakeholders. The earliest draft of the standard contained 380 total practices drawn from a wider range of cybersecurity guidance documents,

whereas the January 2020 CMMC standard contained 171 total practices drawn primarily from NIST Special Publication 800-171.

The CMMC program office also coordinated with other DOD components in the development of aspects of the framework. Specifically, program officials said they worked with DIBCAC, leveraging its experience conducting cybersecurity assessments similar to CMMC level 3 assessments. DIBCAC officials told us that they shared lessons learned with the program office and contributed to the development of CMMC training, among other things. Officials from DOD's Office of the Chief Information Officer said they worked with the program office to refine the list of practices in the initial standard and to ensure consistency with existing cybersecurity standards and departmental policies. In addition, officials from the Office of the Under Secretary of Defense for Intelligence and Security, which manages DOD's overall CUI program, said the program office had played in important role in bringing a range of DOD organizations together to build consensus around cybersecurity requirements.

Further, DOD conducted a series of activities beginning in April 2020 as part of a CMMC pathfinder effort—a series of exercises to test the certification process—intended to identify and reduce risks related to CMMC implementation. The pathfinder included simulated assessments of a DIB company under an existing DOD contract and the DIB company's subcontractors. CMMC program officials said that the pathfinder effort helped inform the development of guidance documents, including the CMMC assessment guides and sample contract language.

On November 4, 2021, DOD announced the release of CMMC 2.0, which includes a number of significant modifications to the initial CMMC framework and standard in place at the time of our audit. For example, according to DOD's CMMC website, CMMC 2.0 eliminates levels 2 and 4, a number of CMMC-unique practice requirements, and all maturity process requirements. The website indicates that the remaining three levels—foundational, advanced, and expert—are equivalent or similar to levels 1, 3, and 5 under the initial framework and standard.

DOD CMMC documentation indicates that for the new level 1 (foundational), a company will no longer be required to pass an external assessment to achieve certification. Instead, companies will have to submit an annual self-assessment to achieve and maintain level 1 certification. For the new level 2 (advanced), DOD indicated some companies will still be required to pass a third-party assessment to

achieve certification; however, the assessment criteria will be based solely on all 110 practices in NIST Special Publication 800-171. For the new level 3 (expert), CMMC documentation notes that companies will be required to pass a government-led assessment to achieve certification. According to DOD, requirements for level 3 are planned to include all 110 practices in NIST Special Publication 800-171 and a subset of practices in NIST Special Publication 800-172. However, with these modifications to the framework and standard, DOD did not state when the requirements for level 3 will be finalized.

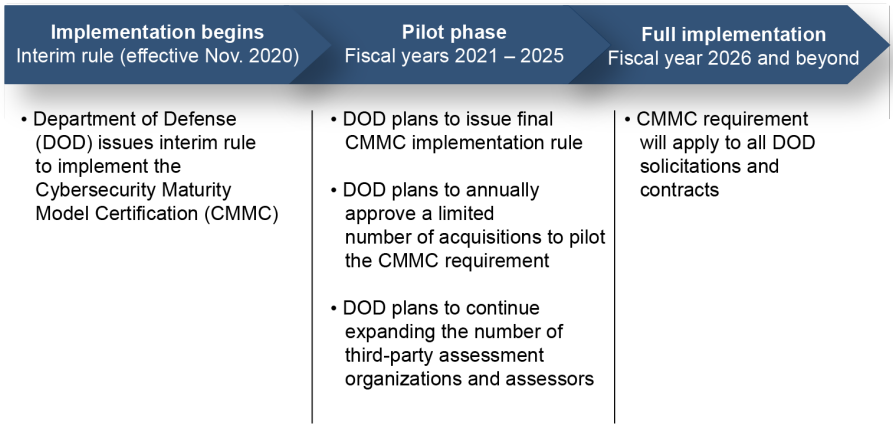
DOD Has Not Met Initial Implementation Goals or Sufficiently Communicated Key Decisions to Industry

DOD began implementing CMMC in September 2020 through an interim rule (effective November 30, 2020) and is currently in the 5-year pilot phase leading to full CMMC implementation. However, implementation of the pilot has been delayed and the program has not met its fiscal year 2021 goals. DIB companies have also expressed a broad range of concerns about CMMC implementation, such as costs to support assessments, reciprocity with other cybersecurity certifications, and assessment consistency. While DOD initially engaged with DIB companies and trade groups in refining early versions of the CMMC model, it has since not provided sufficient and timely communication to industry on implementation details due to several factors cited by the department, such as communication limitations imposed by the rulemaking process.

DOD Has Taken Steps to Implement CMMC and Expects Full Implementation in Fiscal Year 2026

DOD plans to roll out CMMC over a 5-year period, beginning with initial implementation in 2020, followed by a 5-year pilot phase leading to full implementation in fiscal year 2026. Figure 3 shows a time line of DOD's key CMMC implementation activities.

Figure 3: Overview of DOD's Implementation Plan for CMMC and Key Activities, as of October 2021



Source: GAO summary of DOD's CMMC implementation activities. | GAO-22-104679

Note: Information in this figure is current as of October 2021. In November 2021, DOD released CMMC 2.0, which includes a number of significant modifications to the initial framework and standard.

CMMC Implementation Began with Interim Rule

In September 2020, DOD issued an interim rule (effective November 30, 2020) that amended the DFARS to establish DFARS clause 252.204-7021,[22] which requires the contractor to:

- hold a current CMMC certification at the level required by the solicitation and contract,[23]
- maintain the certification for the duration of the contract, and
- flow-down CMMC certification requirements to subcontractors at all tiers to ensure that each subcontractor has a current (i.e., not older than 3 years) certificate at the level that is appropriate for the information that is being flowed down to the subcontractor.

The Office of the Under Secretary of Defense for Acquisition and Sustainment must approve the use of a CMMC requirement in any

[22]85 Fed. Reg. 6, 1505, Interim rule, (Sept. 29, 2020) (effective Nov. 30, 2020).

[23]Through fiscal year 2025, DFARS clause 252.204-7021 is prescribed for use in solicitations and contracts or task order or delivery orders, including those for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of commercially available off-the-shelf items, if the requirement document or statement of work requires a contractor to have a specific CMMC level.

solicitation during the pilot period (through fiscal year 2025). According to CMMC program officials, DOD plans to release additional information in November 2021 about its plans for finalizing the DFARS interim rule.

DOD Plans to Increase CMMC Adoption over 5-Year Pilot Phase, but Faces Delays

DOD plans to roll out CMMC implementation over a 5-year period, referred to as the pilot phase. This phase includes annual implementation goals for the number of acquisitions that will include CMMC as a contract requirement, increasing from up to 15 acquisitions in fiscal year 2021 to up to 479 acquisitions in fiscal year 2025. During the pilot phase, a company competing for a CMMC pilot contract will need to be assessed and certified at an appropriate level, depending on the sensitivity of the information associated with a program or technology being developed, to be eligible for the contract award. In its January 2021 report to Congress, DOD identified 11 acquisitions nominated by service and component acquisition executives to participate in the CMMC pilot during fiscal year 2021.

However, DOD has fallen behind in meeting its pilot implementation goals. Specifically, no acquisitions included CMMC as a contract requirement in fiscal year 2021. DOD and the CMMC-AB have made only limited progress certifying the third-party organizations that will conduct CMMC assessments. As of November 2021, according to CMMC-AB data, there are five fully certified assessment organizations and more than 190 potential assessment organizations that are awaiting a DIBCAC assessment. As a result, no DIB companies, other than assessment organizations, have been assessed.[24]

According to CMMC program officials, DOD has not yet released a list of the specific acquisitions that will be included in the CMMC pilot for fiscal year 2022 and beyond. The officials said that the Under Secretary will issue a memorandum near the beginning of each fiscal year that defines the target pilot acquisitions for that year. This approach, according to

[24]In preparing the interim rule, DOD estimated the total number of assessments needed to support CMMC implementation by assuming that there are approximately 100 unique subcontractors for every unique prime contractor. Therefore, the total number of assessments—covering both prime contractor and subcontractor—required to support the pilot programs increases from 1,500 the first year to about 47,900 in the fourth and fifth years. Renewal of the certifications, which must occur every 3 years, are not included in these estimates.

program officials, is intended to help ensure that supporting elements of CMMC, such as certified assessment organizations and trained assessors, are in place to support the acquisitions that will include CMMC as a requirement at contract award.

The DIB Has Expressed a Broad Range of Concerns about Details of CMMC Implementation and Requirements

Between September and November 2020, DOD received 189 public comments on the DFARS interim rule expressing concerns about various aspects of how CMMC will work.[25] CMMC program officials noted that they are adjudicating DOD's responses to these concerns as part of the rulemaking process. A number of these concerns were also raised in our discussions with DIB companies. Examples of the concerns cited in public comments on the DFARS interim rule and in one or more of our discussions with selected industry organizations, including group discussions, follow.

- Plans of Action and Milestones (POAM): Participants during group discussions with both large and small defense contractors expressed concerns with DOD's decision not to allow POAMs under the current CMMC framework. Under other cybersecurity assessment processes, a company may describe its plans to address any identified deficiencies with a POAM, which outlines specific activities and time lines.[26] CMMC currently prohibits third-party assessment organizations from accepting a company's POAM as a substitute for addressing an identified deficiency. In public comments on the DFARS interim rule, one organization said that not allowing POAMs prevents organizations from managing deficiencies properly. DIBCAC officials told us that from their experience, few companies generally demonstrate compliance with all requirements during an assessment. Specifically, according to DIBCAC officials, of the 110 companies DIBCAC assessed between fiscal years 2019 and 2020, about 16

[25]According to the CMMC program, some of the comments were multi-page inputs covering a range of different topics or "items" and there was a total of more than 800 items in the public comments.

[26]Organizations may develop and implement POAMs based on findings from security control assessments, security impact analyses, continuous monitoring of activities, audit reports, and other sources.

percent satisfactorily demonstrated that they were meeting all requirements. Those officials later told us that as of October 2021, with data from subsequent assessments, this number had increased to about 22 percent.

- Reciprocity: DOD has not yet defined how CMMC will incorporate reciprocity. Representatives from DIB companies expressed concerns that DOD had not yet defined reciprocity between CMMC and other types of cybersecurity certifications. Reciprocity aims to reduce the costs associated with preparing for and supporting two or more assessments that require a company demonstrate compliance with similar types of requirements or standards. In public comments on the DFARS interim rule, one commenter said that without clear reciprocity between CMMC and other types of cybersecurity assessments, a company may need to comply with multiple, overlapping standards to maintain eligibility to compete for DOD contracts. During our discussion group with small defense contractors, participants said that it is critical for CMMC to include reciprocity with other federal requirements, such as FedRAMP, that companies have already implemented. These representatives said that without reciprocity, the duplicative compliance costs will be a burden for DIB companies, particularly small businesses.
- Resources required for assessments: Comments on the DFARS interim rule said that DOD's analysis underestimated CMMC compliance costs. For example, in the DFARS interim rule, DOD estimated that a contractor could calculate and submit a CMMC self-assessment in 45 minutes at a cost of around $74. However, one comment noted that companies would spend more time on activities to validate the results of their self-assessment, such as reviewing supporting documentation. Similarly, representatives from a DIB company that has gone through a DIBCAC assessment, which covers about 83 percent of the practices covered by a CMMC level 3 assessment, said their costs to support the assessment were much higher than DOD's estimate of 420 labor hours per assessment. Representatives from this company we spoke with said they invested 3,600 hours of staff time to support their DIBCAC assessment.
- Assessment consistency: Industry and members of the CMMC ecosystem expressed concern about the consistency of assessments across assessment organizations. During our discussion group with small defense contractors, participants told us that each practice is subject to interpretation and DOD has not provided sufficient guidance on how the practices should be assessed. They also said that without additional guidance, any company could fail an assessment

depending on how an assessor interprets each practice. In public comments on the DFARS interim rule, one commenter stated that assessors will have to apply subjective judgements about what is sufficient to adequately address a requirement. Representatives from DIB companies that conduct cybersecurity assessments we spoke to raised similar concerns. The officials said DOD has not provided standards for evaluating evidence during an assessment. They noted that the current assessment guides identify the types of evidence that assessors should consider but do not identify how they are to interpret the evidence. As a result, two different assessors could look at the same evidence and come to different conclusions.

- Appeals process: Industry officials have also expressed concerns with the CMMC appeals process and the role of the CMMC-AB in that process. Specifically, during our discussion group with large defense contractors, the group noted that the DFARS interim rule does not provide enough detail on how the CMMC framework will handle disputes between DIB companies and third-party assessment organizations. They told us that they would like DOD to clarify the standards, processes, and responsibilities for adjudicating disputes. This group also told us that they are concerned about the extent to which the CMMC-AB will adjudicate and oversee the appeals process, given that the members of the CMMC-AB may be employees of competitor defense contractors. Representatives told us they would like clarity on how disputes are ultimately resolved, including whether independent arbitration would be possible. Additionally, group members stated concern about the time it may take to go through the appeals process potentially affecting their ability to compete for DOD contracts. Further, in comments to the interim rule, one organization stated that the rule does not provide enough details on the process to appeal adverse determinations and DOD should identify the options available to DIB companies that may fail an assessment. Another commenter stated that they were unsure of their ability to appeal CMMC assessment determinations with DOD because the CMMC-AB is a nongovernment entity and as a result, they would like more clarity on their options to appeal an assessment.
- Impact on small business: Industry representatives have expressed concerns about the impact of CMMC on small businesses. In public comments on the DFARS interim rule, one commenter stated that the speed at which DIB companies will need to be compliant with CMMC requirements will impede the ability of small businesses to compete for DOD contracts. Specifically, the commenter noted that due to the low number of approved assessors, those assessment organizations that are certified might first focus on large DIB companies at the

expense of small businesses. During our discussion group with small defense contractors, a participant told us that small businesses may consider the added cost and competitive uncertainty as incentives to exit the government contracts marketplace. Further, in a 2019 feasibility review of NIST Special Publication 800-171 requirements for small businesses, MITRE reported that small businesses are hindered in their ability to meet the requirements because they may lack the expertise to interpret the requirements and resources needed to fund the technology solutions.

During the course of this audit, we discussed a range of other topics and issues with both government and industry representatives that are important to the design and implementation of CMMC. One such example is the categorization of CUI information by DOD. See appendix II for additional topics and issues related to CMMC that were raised in discussions with government and industry representatives.

DOD Has Not Communicated Information on Issues Related to CMMC Implementation

DOD Has Not Provided Sufficient or Timely Communication on Issues Related to CMMC Implementation

Industry officials have said that since DOD released the initial CMMC standard in January 2020, the department's communication on aspects of CMMC implementation has been deficient. Our analysis also found that, while DOD has been offering updates on the implementation of CMMC to contractors through social media and webinars, those updates have not included sufficient details for implementation desired by contractors. As a result, representatives from DIB companies, both large and small, told us that they do not know how to prepare for CMMC. Representatives from a research center involved in the development of CMMC said that, from the beginning of the process, the expectation among stakeholders was that DOD would provide written guidance to supplement the CMMC standard and assessment guides. These representatives noted, however, that there has not been enough DOD guidance on specific areas of implementation.

Standards for Internal Control in the Federal Government state that management should externally communicate quality information to achieve the entity's objectives. Specifically, management should select appropriate methods to communicate externally and consider a variety of factors in selecting an appropriate method of communication, including

the needs of the audience and any legal or regulatory requirements, and should ensure that the organization has the appropriate tools to communicate quality information on a timely basis.[27]

Two issues, reciprocity and scoping, provide examples of how DOD's communication to industry has not been sufficient or timely. Specifically, for these issues, DOD has not provided sufficient information to companies about when to expect clarification on issues companies and the department have raised.

- Reciprocity. CMMC program officials have described in public forums, including on their website and in press articles, the intention to provide clarity on the details surrounding reciprocity between CMMC and other assessment regimes, including FedRAMP. Given that the CMMC framework incorporates other cybersecurity standards, particularly NIST Special Publication 800-171, program officials have stated their intention to allow reciprocity with assessments that also leverage those standards. In a January 2021 report to Congress, DOD stated that it was in the process of finalizing reciprocity between CMMC and DOD assessments that use NIST Special Publication 800-171 and that it was coordinating reciprocity agreements between CMMC and FedRAMP.

  However, as of October 2021, the CMMC program office had not released any further details on reciprocity, and DOD officials told us in August 2021 that they do not expect to address reciprocity in the DFARS final rule but would address it in future rulemaking at some point.
- Assessment scoping. DOD has not yet communicated an updated timeline to the DIB on when it plans to provide information on the scoping of assessments for CMMC levels 1 and 3. Scoping helps define the systems, networks, and equipment that will be included in an assessment. While DOD issued assessment guides for levels 1 and 3 in November 2020, as discussed above, those documents stated that guidance on assessment scoping would be included in subsequent updates. Two industry representatives that were part of a working group that supported the assessment scoping guidance said progress on the guidance and communication from the program office slowed in early 2021 and then stopped around April 2021. Individuals

[27]GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

that received training as CMMC assessors said that scoping is a key consideration that will drive assessment costs. Representatives from a research and development center who were involved in the development of CMMC said they raised concerns in 2019 about the lack of scoping guidance with CMMC programs officials. In June 2021, program officials told us that the guidance was under technical review and that they would soon finalize and issue guidance on how to scope CMMC assessments. However, as of October 2021, the program office had not yet posted this information on its website.

- Small business concerns. DOD has emphasized the desire to support small businesses— which represent about three-quarters of the companies expected to get a certification—in meeting the requirements for CMMC. During our discussion group with small defense contractors, participants said they have been unable to get answers to questions needed to prepare for their assessments. For example, one representative told us they have been unable to obtain sufficient information on when assessment organizations will be certified to begin assessing DIB companies. Other participants said they need more information and guidance from DOD on specific technical questions. Not having sufficient information around technical issues that may determine the results of an assessment makes it challenging for DIB companies to understand their responsibilities, prepare for assessments, and estimate associated costs.

The absence of sufficient and timely information is reflected by the CMMC program office's public web site, which has not been updated in more than 10 months. The program office developed a website that includes pages for updates and frequently asked questions (FAQ) to communicate information about implementation to contractors. However, the website was last updated in December 2020 and has not included any updates through October 2021, including information on subsequent changes in the implementation of CMMC. For example, the website's "Updates" page does not include any new information since the September 2020 DFARS interim rule. Similarly, the program office's "FAQ" page lists DOD's planned number of acquisitions to include in its CMMC pilot for fiscal year 2021, though as noted above, program office officials have said that the planned rollout is not on schedule and no contracts included the requirement in 2021.

DOD Faces Communication Limitations from Rulemaking and Staffing Challenges

CMMC program officials said that they have engaged with and communicated information to the DIB in a variety of ways but have faced limitations due to the rulemaking process, a DOD internal review of CMMC, and limited staffing resources. Specifically, the officials said they are unable to comment on certain aspects of CMMC, such as plans for reciprocity, while rulemaking is underway. As noted above, the officials anticipate that DOD will release additional information about its plans to finalize the DFARS interim rule in November 2021. The public comment period, as the term suggests, is for the public to provide comments, scientific data, expert opinions, and facts on the interim rule for the agency to base its reasoning and conclusions on the rulemaking record. While DOD is involved in the rulemaking process, the department's communication with its DIB partners on time frames and similar information remains important.

In March 2021, the Deputy Secretary of Defense directed an internal review of the CMMC program. While the internal review team has completed its analysis and briefed both DOD and congressional staff, CMMC program officials noted that the department had not yet determined how it will address the recommendations and what changes, if any, it will make to CMMC. Program officials said they expect those decisions to be made in late 2021, prior to the issuance of the DFARS final rule.

In addition, program officials said the program office has not had enough staff to handle all its communication demands. Specifically, program officials noted that, as of August 2021, they had only two full-time staff. The officials further noted that they have ongoing efforts underway to hire two more senior staff with expertise in project management and cybersecurity to carry out CMMC program goals. They also said that they are reviewing program office resource and staffing needs as part of the fiscal year 2023 budget cycle.

On November 4, 2021, DOD announced the release of CMMC 2.0, which includes a number of significant modifications to the initial CMMC framework and standard, as discussed above. According to its CMMC website, DOD stated that it plans to implement the revised rules for CMMC through the rulemaking process with new public comment periods. In addition to reducing the number of companies that must pass an external assessment to receive CMMC certification, under CMMC 2.0,

DOD plans to allow POAMs to achieve certification in some circumstances and plans to develop a waiver of CMMC requirements for certain mission-critical needs. DOD also indicated it intends to use rulemaking to implement reciprocity for CMMC by clarifying acceptance agreements with other cybersecurity standards and assessments.

DOD Has Not Established Measures to Monitor and Ensure Success of CMMC

DOD's plan to roll out the CMMC pilot does not reflect GAO's leading practices for designing a pilot, and the department does not yet have a plan in place that would position DOD to evaluate CMMC's effectiveness at meeting its goals. DOD has defined some objectives and data collection activities for its pilot, but the pilot is not designed to provide DOD the means to measure performance against its goals. In addition, DOD also has not yet developed outcome-oriented performance measures to determine the extent to which CMMC is meeting DOD's overall goals to increase the security and resiliency of the DIB and to provide greater assurance that companies can adequately protect FCI and CUI at a level commensurate with the risk.

DOD's CMMC Pilot Does Not Reflect All Leading Practices

DOD's plan to pilot CMMC requirements on a limited number of contracts does not reflect all GAO leading practices for effective pilot design.[28] Key practices include:

[28]GAO's leading practices for effective pilot design include two additional criteria that are not included in this analysis: (1) develop a detailed data-analysis plan to track the pilot program's implementation and performance and evaluate the final results of the project and draw conclusions on whether, how, and when to integrate pilot activities into overall efforts, and (2) ensure appropriate two-way stakeholder communication and input at all stages of the pilot project, including design, implementation, data gathering, and assessment. We determined that that the first of these criteria was not applicable because DOD had not completed the preceding step to clearly articulate assessment methodology and a data gathering strategy. We determined that the second of these criteria was already addressed by our earlier analysis of DOD's communication on CMMC. GAO, *Data Act: Section 5 Pilot Design Issues Need to Be Addressed to Meet Goal of Reducing Recipient Reporting Burden*, GAO-16-438 (Washington, D.C.: Apr. 19, 2016).

- Establish well-defined, appropriate, clear, and measurable objectives. Such objectives should have specific statements of the accomplishments necessary to meet the objectives. Clear and measurable objectives can help ensure that appropriate evaluation data are collected from the outset of pilot implementation so that data will subsequently be available to measure performance against the objectives. Broad study objectives should be translated into specific, researchable questions that articulate what will be assessed.
- Clearly articulate an assessment methodology and data gathering strategy that addresses all components of the pilot program and include key features of a sound plan. Key features of a clearly articulated methodology include a strategy for comparing the pilot implementation and results with other efforts, a clear plan that details the type and source of the data necessary to evaluate the pilot, and methods for data collection including the timing and frequency.
- Identify criteria or standards for identifying lessons about the pilot to inform decisions about scalability and whether, how, and when to integrate pilot activities into overall efforts. The purpose of a pilot is generally to inform a decision on whether and how to implement a new approach in a broader context. Therefore, it is critically important to consider how well the lessons learned from the pilot can be applied in other, broader settings. To assess scalability, criteria should relate to the similarity or comparability of the pilot to the range of circumstances and population expected in full implementation. The criteria or standards can be based on lessons from past experiences or other related efforts known to influence implementation and performance as well as on literature reviews and stakeholder input, among other sources.

DOD's Pilot Has Not Established Well-Defined, Appropriate, Clear, and Measurable Objectives

DOD has defined objectives for the CMMC pilot, including the implementation goals discussed above, but has not incorporated the leading practice for effective pilot design to establish well-defined, appropriate, clear, and measurable objectives that include specific statements of the accomplishments necessary to meet the objectives. For example, the federal register notice for the DFARS interim rule states that the pilot is intended to minimize financial impacts, especially for small businesses, and disruption to the existing DOD supply chain. In August 2020, the then-Under Secretary of Defense for Acquisition and Sustainment wrote that the pilot is intended to ensure a smooth transition for DOD and the DIB during implementation of CMMC. However, neither

the federal register notice for the DFARS interim rule, CMMC documents, nor memorandums announcing the start of the pilot include any statements defining how the pilot will demonstrate its success against those goals. Similarly, DOD has not yet stated how the specific pilot acquisitions selected to date support its goals, such as by specifying a portion of acquisitions that must include small businesses as contractors or subcontractors.

According to leading practices, effective pilot design begins with the establishment of well-defined, appropriate, clear, and measurable objectives that include specific statements of the accomplishments necessary to meet the objectives. DOD's statements about the intent of the CMMC pilot are important for defining its overall objectives. However, without measurable objectives, DOD may not be able to effectively evaluate the CMMC pilot, including the extent to which the pilot is supporting its goals to minimize the financial impacts of CMMC implementation for small businesses.

DOD Does Not Have a Plan for How It Will Utilize Data Collected During the Pilot

DOD has planned data collection activities during the 5-year CMMC pilot but has not incorporated the leading practice for pilot design to develop a detailed plan to organize and use its data collection activities to track the pilot's implementation and performance and to evaluate its results. Specifically, program officials said they intend to use pre- and post-assessment forms to capture data on the plans for and the results of assessments during the pilot, respectively. The program office stated that these data will support metrics and oversight, quality control, and cyber incident analyses, among other things, but has not defined when and how those analyses will be conducted or how the program office plans to use the results to measure the pilot's implementation and performance. For example, for each practice or process associated with a given CMMC level, the post-assessment form requires the CMMC assessor to identify the types of evidence they assessed, the amount of time spent assessing the practice or process, and the contractor's score. Program officials said collecting this data will allow them to identify and track some potential issues, such as which individual practices or processes are most likely to cause an organization to fail its assessment. The post-assessment also includes space for both the assessor and the contractor under assessment to enter recommendations for improving assessment guidance and descriptions.

While such data collection activities are necessary to assess the pilot's performance, the program office has not defined a detailed plan to organize and use the data, such as how it will determine that the data are reliable and how it will conduct its analyses. Without a detailed plan to use the data collected, DOD will not know whether the data collected are sufficient to help the program office effectively evaluate the implementation of the pilot.

DOD Has Not Defined How the Pilot's Design Will Identify Criteria to Inform Decisions about Overall CMMC Efforts

DOD's design for the CMMC pilot does not reflect the leading practice for pilot design to identify criteria or standards for identifying lessons about the pilot to inform decisions about scalability and whether, how, and when to integrate pilot activities into overall efforts. The leading practice states the criteria or standards should be observable and measurable events, actions, or characteristics that provide evidence the pilot has met or is meeting its objectives. The purpose of a pilot, according to the leading practice, is generally to inform a decision on whether and how to implement a new approach in a broader context.

By contrast, DOD has, in the interim rule, communicated its intent to apply CMMC to all solicitations and contracts including those for the acquisition of commercial items (except those exclusively for commercially available off-the-shelf items) valued at greater than the micro-purchase threshold, starting in fiscal year 2026. Such statements raise questions about the extent to which the CMMC pilot is intended to inform decisions about whether to integrate the requirement more broadly. Further, DOD has not defined how it will identify or use lessons learned from the pilot to improve CMMC as it applies the requirement more broadly.

Given that DOD plans to establish annual implementation targets and define specific acquisitions for the pilot at the beginning of each fiscal year, the department has regular opportunities during the pilot to modify its design and implementation. Therefore, even if DOD pursues full implementation of CMMC regardless of the pilot's results, the department may still modify the design of its pilot in subsequent years to incorporate criteria or standards for identifying lessons for how to modify CMMC, as needed, so that it can successfully scale to increasingly larger numbers of acquisitions. Without criteria or standards for identifying lessons about the pilot, DOD may lose an opportunity to better understand and address the challenges associated with scaling up the pilot from its plans for 7,500

assessments in fiscal year 2022 to the more than 90,000 assessments—both new certifications and renewal of certifications—needed to support full implementation.

DOD Does Not Have a Plan to Evaluate the Effectiveness of CMMC

CMMC is part of DOD's efforts to develop a comprehensive framework to enhance cybersecurity for the DIB in response to Congress's direction.[29] Congress required the Secretary of Defense to develop quantitative metrics, among other things, to assess the effectiveness of the overall framework over time at reducing the loss of CUI from the DIB. CMMC's goal is to increase the security and resiliency of the DIB and to provide greater assurance that companies can adequately protect FCI and CUI at a level commensurate with the risk. Knowing whether CMMC is achieving results, such as by measuring the extent to which CMMC is reducing the risk to DOD's sensitive unclassified information, is an important element of the entire effort.

Our prior work and federal guidance also highlight the importance of assessing the effectiveness of program, policies, and organizations against their intended goals.[30] Specifically, GAO guidance states that program evaluation is key to learning and improvement and can be used to determine the extent to which a program, process, or activity is being implemented as intended. As part of program evaluation, agencies can conduct an outcome evaluation to measure the extent to which a program, policy, or organization has achieved its intended outcome(s) and focuses on outputs and outcomes to assess effectiveness.[31] While a range of measures are important, measures of outcomes, not outputs, are

[29]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116–92, § 1648.

[30]GAO, *Performance Measurement and Evaluation: Definitions and Relationships,* GAO-11-646SP (Washington, D.C.: May 2, 2011); and *Program Evaluation: Key Terms and Concepts*, GAO-21-404SP (Washington, D.C.: Mar. 22, 2021). Office of Management and Budget, *Phase 4 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Program Evaluation Standards and Practices,* Memorandum M-20-12 (Washington. D.C.: Mar. 10, 2020); and *Circular No. A-11, Preparation, Submission, and Execution of the Budget* (Washington, D.C.: July 1, 2021).

[31]GAO-11-646SP and Office of Management and Budget Memorandum M-20-12 and Circular No. A-11 state that performance measures may address the type or level of program activities conducted (process), the direct products and services delivered by a program (outputs), or the results of those products and services (outcomes).

the key set of measures and should be used where feasible and appropriate.

DOD has taken some initial steps to collect output data on CMMC but does not have a plan to assess CMMC's effectiveness with outcome-oriented performance measures. DOD is planning to collect data from the CMMC assessment organizations regarding the implementation of the pilot. DOD officials told us that they are also tracking data on the implementation of CMMC, such as the number of trained assessors and certified third-party assessment organizations. Although the data collected are helpful in determining outputs, it is only one type of performance measure. Only assessing CMMC's output does not put DOD in a position to evaluate CMMC's effectiveness.

Performance measures can be used to describe how CMMC's goals are to be achieved, help assess the status of CMMC, identify areas that need improvement, and ensure accountability for end results. For example, potential outcome measures for CMMC could assess reduced risk to DOD's sensitive information or fewer instances of DOD data exfiltrated from DIB company networks. Developing such measures would better position DOD to evaluate the extent to which CMMC is meeting the department's goal to increase the security and resiliency of the DIB, and to course-correct if needed.

CMMC program officials stated that they have not developed a plan that they could use to assess the effectiveness of CMMC because they are focused on designing and implementing the pilot and have had only initial conversations to plan for and identify the type of data they plan to collect. Focusing on the implementation of the CMMC pilot is prudent. However, a key aspect of that focus is planning for and identifying the types of outcome measures that will be needed to assess CMMC's effectiveness, which will help DOD assess its achievement towards its goals. Without establishing a plan that includes performance measures, it will be difficult for DOD to determine whether it is achieving the intended goals and areas that need improvement.

On November 4, 2021, DOD announced that it intends to suspend the current pilot while rulemaking efforts are underway to implement CMMC 2.0.

Conclusions

DOD developed CMMC to increase the cybersecurity posture of the DIB, which has long been a target of—and has become increasingly vulnerable to—cyber intrusion and attacks. The success of CMMC relies on DIB companies implementing and maintaining key cybersecurity practices and processes as well as DOD's ability to effectively design and execute the CMMC verification process. As DOD works to fully define and implement additional changes to CMMC, clear communication of details, including timely updates on key aspects of CMMC requirements and verification processes, would help DIB companies better prepare for certification. Additionally, with CMMC still in early stages, DOD can benefit from having plans to better assess the outputs of the pilot in meeting DOD's implementation goals as well as to assess the outcomes of the overall effort in supporting the department's strategic goals. Without such plans, DOD risks not knowing the extent to which CMMC is meeting the department's strategic goals of improving DIB cybersecurity.

Recommendations for Executive Action

We are making three recommendations to the Department of Defense:

The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment provides sufficient and timely communication to industry on Cybersecurity Maturity Model Certification, including when additional information will be forthcoming. (Recommendation 1)

The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment develops a plan to evaluate the effectiveness of Cybersecurity Maturity Model Certification's pilot, including establishing measurable objectives, collecting relevant data, and identifying lessons and plans to use that information to inform future decisions about the Cybersecurity Maturity Model Certification. (Recommendation 2)

The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment develop outcome-oriented performance measures to evaluate the effectiveness of Cybersecurity Maturity Model Certification as a component of the department's efforts to enhance cybersecurity for the defense industrial base. (Recommendation 3)

Agency Comments and Our Evaluation

We provided a draft of this report to DOD for review and comment. In its comments, reproduced in appendix III, DOD agreed with our recommendations and announced plans to address them, including through its CMMC 2.0 modifications, which in part address issues raised in this review.

With respect to our first recommendation, to provide sufficient and timely communication to industry, DOD noted it has updated the CMMC website, and announced steps to implement CMMC 2.0 through rulemaking. DOD indicated it has begun initial engagement with congressional staff and industry on the transition to CMMC 2.0, which is a positive development. Going forward, in addition to the formal public comment period as part of rulemaking, the department should continue to provide consistent updates to industry throughout the rulemaking process.

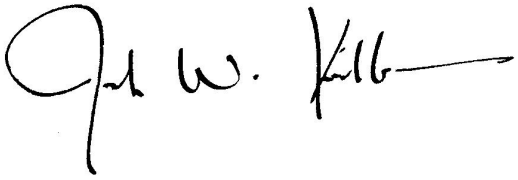
With respect to our second and third recommendations, to develop a plan for evaluation and outcome-oriented performance measures, DOD said the CMMC program office has initiated activities to identify metrics to evaluate implementation and measure performance. These are important steps that will better enable DOD to improve CMMC as it works toward full implementation. DOD also stated that it has not yet determined the specific structure and scope of any pilot under CMMC 2.0, but that it supports this recommendation and agrees to develop a plan to evaluate the effectiveness of CMMC implementation, including any piloting when conducted. As DOD implements CMMC 2.0, to the extent it follows up on efforts to plan for and execute ways to measure the effectiveness of its implementation efforts, overall performance, and the effectiveness of the effort, it will be better positioned to determine if CMMC is accomplishing its original intent.

DOD also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and the Office of the Under Secretary of Defense for Acquisition and Sustainment. In addition, the report will be available at no charge on GAO's website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact us at (202) 512-4841 or russellw@gao.gov; (202) 512-9971 or kirschbaumj@gao.gov; or (404) 679-1831 or franksj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

W. William Russell
Director, Contracting and National Security Acquisitions



Joseph W. Kirschbaum
Director, Defense Capabilities and Management

Jennifer R. Franks
Director, Information Technology and Cybersecurity

List of Committees

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate
The Honorable Jon Tester
Chairman
The Honorable Richard Shelby
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate
The Honorable Adam Smith
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Armed Services
House of Representatives
The Honorable Betty McCollum
Chair
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

The Senate report accompanying a version of the William M. (Mac) Thornberry National Defense Authorization Act (NDAA) for Fiscal Year 2021 included a provision for us to review the Department of Defense's (DOD) implementation of the Cybersecurity Maturity Model Certification (CMMC).[1] This report addresses (1) what steps DOD took to develop CMMC, (2) the extent to which DOD has made progress in implementing CMMC, including communication with industry, and (3) the extent to which DOD has developed plans to assess the effectiveness of CMMC.

For our first and second objectives, we reviewed the language that required DOD to develop a cybersecurity framework for the defense industrial base (DIB) listed in the National Defense Authorization Act for Fiscal Year 2020.[2] Next, we reviewed relevant federal agency documents related to cybersecurity requirements for the DIB and protecting controlled unclassified information (CUI).[3] We also reviewed the Defense Federal Acquisition Regulation Supplement (DFARS) interim rule implementing CMMC and evaluated a sample of the public comments submitted in response to the rule to understand areas of concern.[4] To get a better understanding of the CMMC framework, we reviewed documents

[1]Senate Report 116-236 to accompany a bill on the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283.

[2]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1648. The National Defense Authorization Act for Fiscal Year 2020 directed DOD to develop a framework to enhance the cybersecurity of the DIB that includes identification of unified cybersecurity standards, regulations, metrics, ratings, third-party certifications, or requirements on the DIB for assessing individual contractors' cybersecurity posture.

[3]Those documents included DOD Instruction 5200.48, Controlled Unclassified Information (CUI), DOD 5000.90, Cybersecurity for Acquisition Decision Authorities and Program Managers, National Institute of Standards and Technology (NIST) Special Publication 800-171 *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organization,* and NIST SP 800-53, *"Security and Privacy Controls for Information Systems and Organizations."*

[4]85 Fed. Reg. 6, 1505, Interim rule, (Sept. 29, 2020) (effective Nov. 30, 2020). We also reviewed DFARS Clause 252.204-7012 *Safeguarding Covered Defense Information and Cyber Incident Reporting* that requires adequate security consistent with NIST Special Publication 800-171 for covered defense information stored on DIB networks.

from DOD, including the January 2021 CMMC report to Congress, CMMC assessment guides, DOD memorandums, and the statement of work detailing the oversight of the CMMC Accreditation Body. Next, we reviewed and compared DOD's efforts to communicate with and provide updates on CMMC to the DIB with leading practices to determine the extent to which DOD's efforts aligned.[5]

Additionally, we met with officials from several DOD components as well as from research and development centers,[6] DIB companies, and DIB trade groups to obtain their perspectives on CMMC development and implementation. Specifically, we conducted separate discussion groups with individual members of a DIB trade group that self-identified either as representing a small defense contractor or a large defense contractor, or as a CMMC assessor or consultant (for a total of three meetings).[7] Each discussion group ranged from 20 to 30 individuals. The discussion groups were conducted from March 2021 to April 2021. The discussion groups were arranged and scheduled by National Defense Industrial Association (NDIA) and the representatives are members of NDIA and were self-selected.[8] During the meetings, GAO asked semi-structured questions that were provided ahead of the meetings and allowed the representatives to provide input to the questions during the meeting. The objective of these meetings was to discuss their perspectives on CMMC and the information received is non-generalizable. Discussion groups are intended to generate in-depth information about the reasons for participants' views on specific topics. The opinions expressed by the participants represent their points of view and may not represent the views of the DIB companies or their leadership. We also met with other industry officials including representatives from DIB companies that have gone through a Defense Contract Management Agency, Defense

[5]GAO, S*tandards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[6]For the purposes of this report, we use the term "research and development centers" to refer to both federally funded research and development centers and university affiliated research centers that were involved in the development of CMMC.

[7]In the report, we refer to these meetings as either (1) discussion group with small defense contractors; (2) discussion group with large defense contractors; and (3 discussion group with CMMC assessors and consultants.

[8]NDIA is a nonprofit, nonpartisan educational association made up of affiliates, chapters, and divisions with about 63,000 members. NDIA engages in dialogue on national security issues by leveraging its members, who represent the military, government, industry, and academia.

Industrial Base Cybersecurity Assessment Center (DIBCAC) assessment, DIB companies that conduct cybersecurity assessments, and DIB trade groups.[9] (For a full list, see below.)

For our third objective, we reviewed DOD documents regarding the implementation of the CMMC pilot including DOD memorandums on the CMMC pilot, the DFARS interim rule implementing CMMC, DOD's CMMC pilot schedule, and recent hearing statements from congressional testimonies related to CMMC. We assessed and compared DOD efforts to implement the CMMC pilot with GAO's leading practices to determine the extent to which DOD efforts were aligned.[10] Additionally, we met with officials from DOD, the CMMC Accreditation Body, and research and development centers to obtain information on the status of the CMMC pilot and its execution and DOD's efforts to collect data to inform future CMMC efforts. We also met with DOD officials to discuss their efforts to evaluate the effectiveness of CMMC. We then compared DOD's efforts with GAO and federal guidance related to evaluation and evidence building.[11]

We met with officials from the below offices within DOD, research and development centers, DIB trade groups, and DIB companies to support all of our objectives:

- Under Secretary of Defense for Acquisition and Sustainment,
- Under Secretary of Defense for Intelligence & Security,
- Department of Defense Chief Information Officer,
- DIBCAC,

[9]To help us better understand the perspectives of DIB companies on cybersecurity assessments, DIBCAC provided a list of companies that had undergone recent DIBCAC assessments and the CMMC Accreditation Body provided a list of companies that conduct cybersecurity assessments. We met with these companies and the information collected is not generalizable.

[10]GAO *Data Act: Section 5 Pilot Design Issues Need to Be Addressed to Meet Goal of Reducing Recipient Reporting Burden,* GAO-16-438 (Washington, D.C.: April 19, 2016)

[11]GAO, *Performance Measurement and Evaluation: Definitions and Relationships*, GAO-11-646SP (Washington, D.C.: May 2, 2011); and *Program Evaluation: Key Terms and Concepts,* GAO-21-404SP (Washington, D.C.: Mar. 22, 2021). Office of Management and Budget, *Phase 4 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Program Evaluation Standards and Practices,* Memorandum M-20-12 (Washington. D.C.: Mar. 10, 2020); and *Circular No. A-11, Preparation, Submission, and Execution of the Budget* (Washington, D.C.: July 1, 2021).

- Defense Logistics Agency, Procurement Technical Assistance Center,
- Carnegie Mellon University, Software Engineering Institute,
- John Hopkins University, Applied Physics Laboratory,
- CMMC Accreditation Body,
- The MITRE Corporation,
- NDIA,
- Professional Services Council,
- DIB Sector Coordinating Council,
- Information Technology Acquisition Advisory Council,
- purposefully selected DIB companies,[12] and
- CMMC assessment organizations.

On November 4, 2021, DOD announced their intention to implement CMMC 2.0, which modifies the initial framework and standard. We used documentary evidence to describe CMMC 2.0 and DOD's plans.

We conducted this performance audit from December 2020 to December 2021 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[12]We met with several groups of DIB company representatives. As discussed above, we had three discussion groups with small and large defense contractors and CMMC assessors and consultants. We also met with representatives from DIB companies that have gone through a DIBCAC assessment and DIB companies that conduct cybersecurity assessments.

Appendix II: Other Topics and Issues for Resolution Raised by Government and Industry

The Department of Defense's (DOD) Cybersecurity Maturity Model Certification (CMMC) is a significant undertaking expected to have broad, lasting effects on companies that are awarded contracts from DOD to provide critical goods and services. During the course of this review, government and industry representatives raised a number of issues that are important to the future course of CMMC. They include:

Sensitive Unclassified Information

- Defining categories of sensitive unclassified information, such as Controlled Unclassified Information (CUI), and correctly marking such information to ensure appropriate handling and safeguarding
- Ensuring acquisition program offices and other DOD entities do not incorrectly mark information that is not sensitive as CUI, which would limit the companies that are eligible to compete for associated contracts

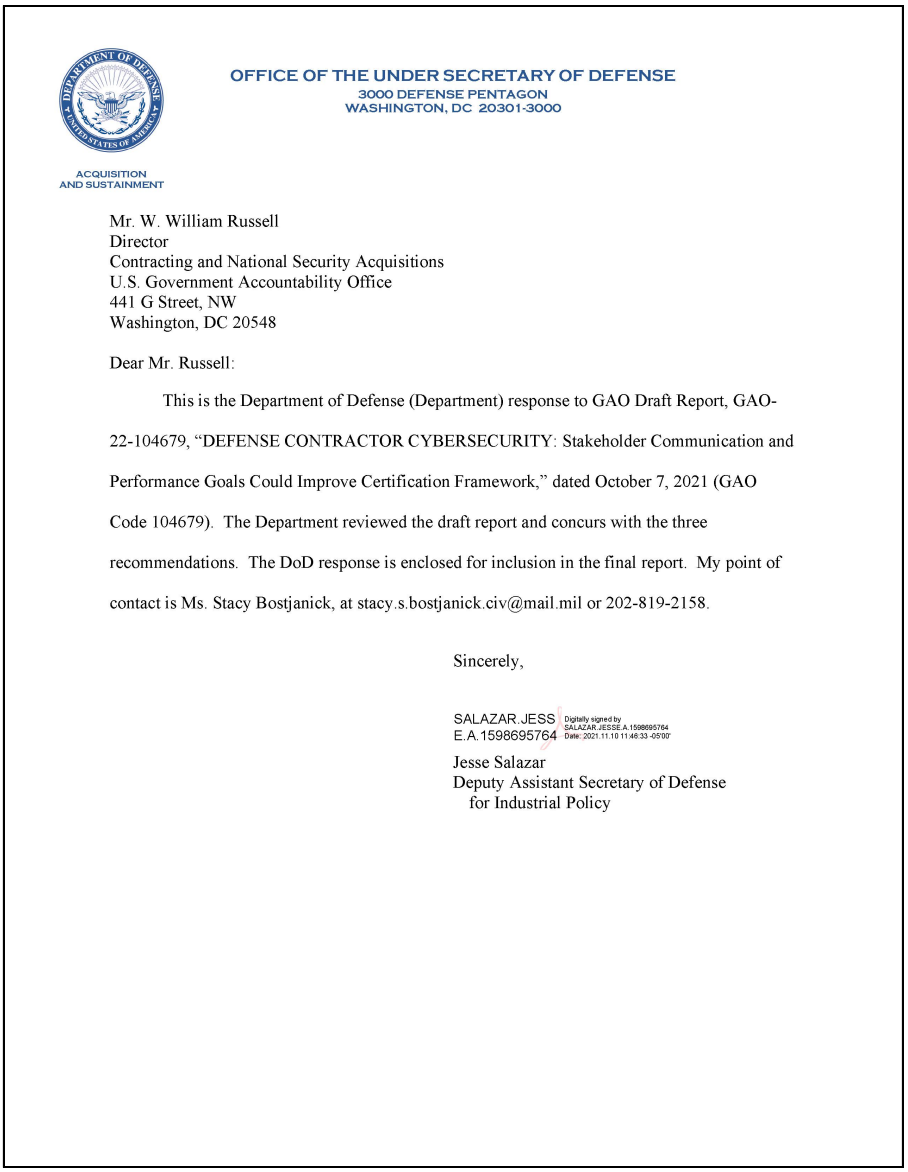
International Company Participation in CMMC

- Determining the extent to which international companies may experience challenges competing under solicitations and performing contracts that include CMMC as a requirement, including timelines and plans for assessment organizations that will assess international companies

CMMC Adoption by Other Federal Agencies

- Monitoring efforts other federal agencies are considering or taking to adopt CMMC or similar requirements for their supply chains

Appendix III: Comments from the Department of Defense



OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACQUISITION
AND SUSTAINMENT

Mr. W. William Russell
Director
Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Russell:

This is the Department of Defense (Department) response to GAO Draft Report, GAO-22-104679, "DEFENSE CONTRACTOR CYBERSECURITY: Stakeholder Communication and Performance Goals Could Improve Certification Framework," dated October 7, 2021 (GAO Code 104679). The Department reviewed the draft report and concurs with the three recommendations. The DoD response is enclosed for inclusion in the final report. My point of contact is Ms. Stacy Bostjanick, at stacy.s.bostjanick.civ@mail.mil or 202-819-2158.

Sincerely,

SALAZAR.JESS E.A.1598695764 Digitally signed by SALAZAR.JESSE.A.1598695764 Date: 2021.11.10 11:46:33 -05'00'

Jesse Salazar
Deputy Assistant Secretary of Defense
for Industrial Policy

GAO DRAFT REPORT DATED OCTOBER 7, 2021
GAO-22-104679 (GAO CODE 104679)

"DEFENSE CONTRACTOR CYBERSECURITY: Stakeholder Communication and Performance Goals Could Improve Certification Framework"

DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment provide sufficient and timely communication to industry on Cybersecurity Maturity Model Certification (CMMC) including when additional information will be forthcoming. (Recommendation 1)

DoD RESPONSE: Concur. On November 4, 2021, the Department issued a formal public announcement on the Strategic Direction for CMMC 2.0, the next iteration of the DoD CMMC cybersecurity model. In conjunction, the updated and improved official CMMC website (https://www.acq.osd.mil/cmmc/index.html) launched on the same day, and includes details of the significant changes incorporated under the new CMMC 2.0 framework and updated Frequently Asked Questions. Additionally, an advanced notice for proposed rulemaking will be posted to the Federal Register in the next week to address the DoD transition to CMMC 2.0 and the required 32 CFR and 48 CFR rulemaking to implement CMMC 2.0. To help build awareness of the notable changes to CMMC, he Department has already initiated external engagements with congressional staff members and industry, whose inputs will be critical to meeting the objectives of the CMMC program. The Department will continue to seek opportunities to engage these stakeholders as we drive towards full implementation.

RECOMMENDATION 2: The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment develops a plan to evaluate the effectiveness of Cybersecurity Maturity Model Certification's pilot, including establishing measurable objectives, collecting relevant data and identifying lessons and plans to use that information to inform future decisions about the Cybersecurity Maturity Model Certification. (Recommendation 2)

DoD RESPONSE: Concur. The CMMC Program Management Office (PMO) has initiated the action to identify suitable and essential metrics from the CMMC program processes to develop a plan for tracking and assessing the data to help evaluate the effectiveness of CMMC implementation. The rollout of CMMC implementation in selected Department acquisitions was delayed in FY2021 after the preliminary CMMC PMO coordination, starting in January 2021, with Services and Components that resulted in 19 DoD acquisition nominations for this first year of the planned five-year phased rollout of CMMC implementation piloting. In March 2021, the Department initiated an internal assessment of CMMC's implementation, informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive 150-day programmatic assessment of CMMC implementation, supported by DoD cybersecurity and acquisition leaders, resulted in several approved CMMC program modifications that together

developed into "CMMC 2.0." The specific structure and scope of any pilot under CMMC 2.0 remains to be determined, but the Department supports this recommendation and agrees to develop a plan to evaluate the effectiveness of CMMC implementation, including any piloting when later conducted.

RECOMMENDATION 3: The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment develop an outcome-oriented performance measures to evaluate the effectiveness of Cybersecurity Maturity Model Certification as a component of the Department's efforts to enhance cybersecurity for the defense industrial base. (Recommendation 3)

DoD RESPONSE: Concur. The Department supports the recommendation to develop outcome-oriented performance metrics that can used to evaluate the CMMC program's effectiveness as a component of the DoD's efforts to enhance DIB cybersecurity. The CMMC Program Management Office is in the process of reviewing the data element set requirements and formally establishing outcome-based performance metrics to measure performance. These metrics will be finalized in conjunction with the formal release of the CMMC 2.0 program in accordance with 32 CFR rulemaking requirements and associated timelines.

Agency Comment Letter

Text of Appendix III: Comments from the Department of Defense

Page 1

Mr. W. William Russell
Director
Contracting and National Security Acquisitions
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Russell:

This is the Department of Defense (Department) response to GAO Draft Report, GAO-22-104679, “DEFENSE CONTRACTOR CYBERSECURITY: Stakeholder Communication and Performance Goals Could Improve Certification Framework,” dated October 7, 2021 (GAO Code 104679). The Department reviewed the draft report and concurs with the three recommendations. The DoD response is enclosed for inclusion in the final report. My point of contact is Ms. Stacy Bostjanick, at stacy.s.bostjanick.civ@mail.mil or 202-819-2158.

Sincerely,

Jesse Salazar
Deputy Assistant Secretary of Defense
for Industrial Policy

Page 2

GAO DRAFT REPORT DATED OCTOBER 7, 2021 GAO-22-104679 (GAO CODE 104679)

"DEFENSE CONTRACTOR CYBERSECURITY: Stakeholder Communication and Performance Goals Could Improve Certification Framework"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment provide sufficient and timely communication to industry on Cybersecurity Maturity Model Certification (CMMC) including when additional information will be forthcoming. (Recommendation 1)

DoD RESPONSE: Concur. On November 4, 2021, the Department issued a formal public announcement on the Strategic Direction for CMMC 2.0, the next iteration of the DoD CMMC cybersecurity model. In conjunction, the updated and improved official CMMC website (https://www.acq.osd.mil/cmmc/index.html) launched on the same day, and includes details of the significant changes incorporated under the new CMMC 2.0 framework and updated Frequently Asked Questions. Additionally, an advanced notice for proposed rulemaking will be posted to the Federal Register in the next week to address the DoD transition to CMMC 2.0 and the required 32 CFR and 48 CFR rulemaking to implement CMMC 2.0. To help build awareness of the notable changes to CMMC, he Department has already initiated external engagements with congressional staff members and industry, whose inputs will be critical to meeting the objectives of the CMMC program. The Department will continue to seek opportunities to engage these stakeholders as we drive towards full implementation.

RECOMMENDATION 2: The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment develops a plan to evaluate the effectiveness of Cybersecurity Maturity Model Certification's pilot, including establishing measurable objectives, collecting relevant data and identifying lessons and plans to use that information to inform future decisions about the Cybersecurity Maturity Model Certification. (Recommendation 2)

DoD RESPONSE: Concur. The CMMC Program Management Office (PMO) has initiated the action to identify suitable and essential metrics from the CMMC program processes to develop a plan for tracking and assessing the data to help evaluate the effectiveness of CMMC implementation. The rollout of CMMC implementation in selected Department acquisitions was delayed in FY2021 after the preliminary CMMC PMO coordination, starting in January 2021, with Services and Components

that resulted in 19 DoD acquisition nominations for this first year of the planned five-year phased rollout of CMMC implementation piloting. In March 2021, the Department initiated an internal assessment of CMMC's implementation, informed by more than 850 public comments in response to the interim DFARS rule. This comprehensive 150-day programmatic assessment of CMMC implementation, supported by DoD cybersecurity and acquisition leaders, resulted in several approved CMMC program modifications that together

Page 3

developed into "CMMC 2.0." The specific structure and scope of any pilot under CMMC 2.0 remains to be determined, but the Department supports this recommendation and agrees to develop a plan to evaluate the effectiveness of CMMC implementation, including any piloting when later conducted.

RECOMMENDATION 3: The Secretary of Defense should ensure the Under Secretary of Defense for Acquisition and Sustainment develop an outcome-oriented performance measures to evaluate the effectiveness of Cybersecurity Maturity Model Certification as a component of the Department's efforts to enhance cybersecurity for the defense industrial base. (Recommendation 3)

DoD RESPONSE: Concur. The Department supports the recommendation to develop outcome- oriented performance metrics that can used to evaluate the CMMC program's effectiveness as a component of the DoD's efforts to enhance DIB cybersecurity. The CMMC Program Management Office is in the process of reviewing the data element set requirements and formally establishing outcome-based performance metrics to measure performance. These metrics will be finalized in conjunction with the formal release of the CMMC 2.0 program in accordance with 32 CFR rulemaking requirements and associated timelines.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

W. William Russell, (202) 512-4841 or russellw@gao.gov

Joseph W. Kirschbaum, (202) 512-9971 or kirschbaumj@gao.gov

Jennifer R. Franks, (404) 679-1831 or franksj@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Raj Chitikila, Nick Cornelisse, and Marisol Cruz Cain (assistant directors); Pete Anderson, Andrew Berglund, Brandon Booth, Breanne Cave, Mary Diop, Keith Kim, Terell P. Lasane, Jamilah Moon, Sylvia Schatz, Roxanna Sun, and Elaine L. Vaurio made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/about/what-gao-does/fraudnet

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548