DEFENSE CONTRACTOR CYBERSECURITY
DOD Should Address External Factors That Could Impede Program Implementation

Report to Congressional Committees

March 2026

GAO-26-107955

United States Government Accountability Office

Accessible Version

GAO Highlights

DEFENSE CONTRACTOR CYBERSECURITY

DOD Should Address External Factors That Could Impede Program Implementation

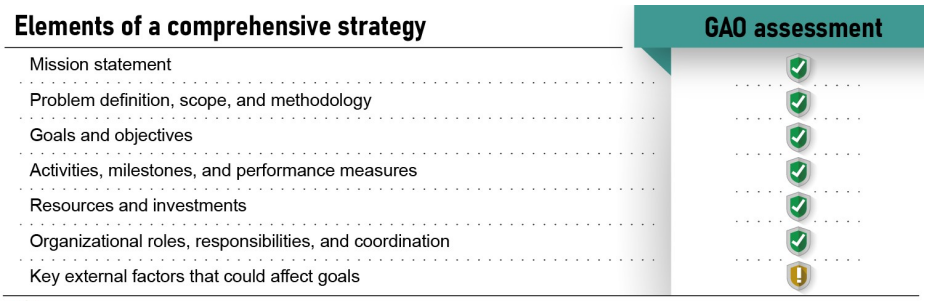
GAO-26-107955
March 2026
A report to congressional committees.
For more information, contact: Joseph W. Kirschbaum at KirschbaumJ@gao.gov; Vijay A. D'Souza at DsouzaV@gao.gov; or W. William Russell at RussellW@gao.gov.

What GAO Found

The Department of Defense (DOD) established the Cybersecurity Maturity Model Certification (CMMC) program in 2020 to ensure that defense industrial base (DIB) companies comply with cybersecurity requirements. In response to concerns about the complexity of the program's initial framework, in 2024 DOD streamlined requirements and revised program implementation plans.

DOD plans to implement this program over the next 3 years. Although DOD does not have a strategic plan for the CMMC program recorded in a single document, it has developed several planning documents to guide implementation. GAO found that DOD's implementation plans addressed six of seven key elements of a comprehensive strategy, as shown in the figure below.

Extent That DOD's Plans for the CMMC Program Rollout Addressed Key Elements of a Comprehensive Strategy, as of September 2025



Sources: GAO analysis of Department of Defense (DOD) information, and all icon illustrations. | GAO-26-107955

DOD partially addressed the element related to identifying key external factors that could affect the program's ability to meet its goals. While DOD has taken steps to develop strategies to address program risks, it has not systematically assessed and documented the external factors that could affect the department meeting its goals. For example, the department relies on private sector stakeholders to conduct assessments of DIB companies to determine if they comply with the program's requirements. However, DOD did not assess and document how it intends to mitigate the risk of private sector capacity being insufficient to meet its needs for assessments, according to DOD officials.

Although DOD officials told GAO that department leaders can issue waivers if external factors cause significant challenges, such waivers would not address underlying challenges. Additionally, depending on the frequency and number of waivers DOD uses, the process could undermine the long-term viability of the CMMC program and its intent to verify that companies are implementing federal cybersecurity requirements. By assessing and documenting key external factors and developing approaches to address them, DOD would better understand program implementation risks and be better positioned to take action to mitigate those risks.

Why GAO Did This Study

DOD relies on hundreds of thousands of private companies for goods and services, ranging from weapon systems to maintenance. In doing business with DOD, these companies often use and store sensitive information in their computer systems. Malicious cyber actors have targeted defense contractors' networks and systems to access sensitive DOD data.

Senate Report 118-188, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2025, includes a provision for GAO to review DOD's implementation of the revised CMMC program. GAO's report evaluates, among other things, the extent to which DOD has a comprehensive strategy to guide implementation.

GAO reviewed DOD's CMMC policies and planning documentation and interviewed DOD officials involved in implementing and managing this program. GAO also interviewed DOD officials and industry representatives who support DIB companies to implement CMMC requirements.

What GAO Recommends

GAO recommends that DOD document key external factors that could significantly affect the CMMC program and develop approaches to address these factors. DOD concurred with the recommendation.

Contents

Abbreviations

CAICO	CMMC Assessor and Instructor Certification Organization
CCA	CMMC Certified Assessor
CCI	CMMC Certified Instructor
CCP	CMMC Certified Professional
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CMMC	Cybersecurity Maturity Model Certification
CMMC-AB	Cybersecurity Maturity Model Certification Accreditation Body
C3PAO	CMMC third-party assessor organizations
CUI	Controlled Unclassified Information
DAU	Defense Acquisition University
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	defense industrial base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DOD	Department of Defense
FAR	Federal Acquisition Regulation
FCI	Federal Contract Information
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OUSD(A&S)	Office of the Under Secretary of Defense for Acquisition and Sustainment
SP	Special Publication

March 12, 2026

Congressional Committees

The Department of Defense (DOD) relies on approximately 200,000 defense industrial base (DIB) private companies for goods and services ranging from weapon systems to maintenance.[1] These companies often use and store sensitive information in their computer systems and face increasing advanced persistent threats from adversaries who seek to access this sensitive information. For example, DOD's *Defense Industrial Base Cybersecurity Strategy 2024* states that malicious cyber activity targeting the DIB can result in the unauthorized access and release of sensitive U.S. government data, proprietary information, and intellectual property.[2] Malicious cyber activity can also result in the destruction of data, inability to conduct business, denial of services, and physical damage to property, according to the *Strategy*. In 2025, the Office of the Director of National Intelligence and the Defense Intelligence Agency reported that nation-state actors were targeting DIB companies to obtain sensitive information.[3]

The U.S. government, through federal regulations, requires nongovernment entities (including but not limited to DIB companies) that have Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) stored, transmitted, or at rest in their systems to meet specific cybersecurity requirements.[4]

Federal Contract Information: Information, 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, but not including information provided by the government to the public (such as that on public websites) or simple transactional information, such as that necessary to process payments.

Controlled Unclassified Information: Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a nonexecutive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

Source: Federal Acquisition Regulation (FAR) clause 52.204-21 and 32 C.F.R. § 2002.4(h) (2016). | GAO-26-107955

[1]DOD also relies on its organic industrial base that includes a network of government-owned industrial facilities, known as depots, which employ over 80,000 civilians and support readiness by maintaining and repairing critical weapon systems for use in training and operations.

[2]DOD Chief Information Officer, *Defense Industrial Base Cybersecurity Strategy 2024* (Mar. 21, 2024).

[3]Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Mar. 18, 2025) and DOD, *DIA 2025 Worldwide Threat Assessment* (May 11, 2025).

[4]Federal Acquisition Regulation (FAR) clause 52.204-21 and Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012.

DOD has promulgated cybersecurity requirements that include adding a clause to contracts to apply these requirements to contractor information systems.[5] However, a 2019 DOD Inspector General report found that DIB companies did not consistently implement the cybersecurity requirements to protect CUI.[6] In response, the department initiated a program that, when implemented, could validate and confirm that DIB companies were in compliance with existing cybersecurity requirements. Specifically, DOD established the Cybersecurity Maturity Model Certification (CMMC) program in 2020 (and subsequently revised it in 2024) to ensure that DIB companies comply with requirements to safeguard FCI and CUI information.[7]

The CMMC program, as established, relies on various stakeholders to execute. For example, DOD contracting officers will help to implement the program through the department's procurement process. It also includes an external accreditation body to oversee CMMC accreditation, certification, training, and assessment processes. DOD currently has a contract with The Cyber AB to fulfill the responsibilities of the accreditation body.[8] Further, DOD's CMMC Program Management Office is to provide oversight of the program and is responsible for establishing assessment, accreditation, and training requirements as well as developing and updating program policies and implementing guidance.

We have previously assessed DOD's efforts to support DIB and small companies in protecting themselves from malicious cyberspace actors. In 2012, we issued a report that examined DOD and private sector efforts to protect the DIB from cyber threats and the extent to which the department had incorporated risk management into its efforts.[9] In 2015, we issued a report that addressed the extent to which DOD's small business office

[5]DOD, *Defense Industrial Base Cybersecurity Strategy 2024*; DOD, Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (October 2016). There are broad ongoing efforts to reform federal and defense acquisitions. Specifically, Exec. Order No. 14,265, 90 Fed. Reg. 15,621 (Apr. 9, 2025) calls for a comprehensive overhaul of the defense acquisition system. In response, the Secretary of Defense and military components are directed to formulate plans to reform acquisition processes and assess major programs. Similarly, another April 2025 executive order directs agencies to streamline the federal acquisition regulations that govern federal procurement. Exec. Order No. 14,275, 90 Fed. Reg. 16,445 (Apr. 15, 2025). In response to Exec. Order No. 14,265, DOD released its Acquisition Transformation Strategy on November 7, 2025. This strategy implements Exec. Order No. 14,265 and describes efforts that are intended to prioritize speed, flexibility, and rigorous execution of acquisition processes. DOD, *Acquisition Transformation Strategy: Rebuilding the Arsenal of Freedom* (Nov. 7, 2025) The FAR and DFAR sections referenced in this report are currently under review and reflect the versions in effect at the time the audit was conducted.

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

[7]DOD, *DFARS Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)*, 85 Fed. Reg. 61,505 (Sept. 29, 2020) (effective Nov. 30, 2020); DOD, *32 C.F.R. Part 170, Cybersecurity Maturity Model Certification (CMMC) Program*, 89 Fed. Reg. 83,092 (Oct. 15, 2024).

[8]The Cyber AB is not an abbreviation. Originally established as the Cybersecurity Maturity Model Certification Accreditation Body Inc. in 2020, it rebranded and has been doing business as The Cyber AB since June 2022. *Memorandum of Understanding Between the Department of Defense and the Cybersecurity Maturity Model Certification Accreditation Body, Inc (CMMC-AB) Regarding CMMC Accreditation, Certification, Approval, Training and Assessment Processes As Related to the Defense Supply Chain (DSC)* (Mar. 23, 2020) (hereinafter CMMC-AB Memorandum of Understanding).

[9]This report was initially restricted from public release since DOD determined that it contained sensitive information and could be disseminated only to persons whose official duties require access to the information. We recommended that the Secretary of Defense take the eight actions in this report. In 2025, DOD cleared the report for public issuance. GAO, *Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats*, GAO-12-762SU (Washington, D.C.: Aug. 3, 2012).

had integrated cybersecurity into its outreach and education efforts to defense small businesses.[10] The department implemented the report's sole recommendation. More recently, in 2021, we assessed DOD's initial effort to roll out CMMC and recommended that the department improve communications to industry, develop a plan to evaluate the effectiveness of the program's pilot, and develop outcome-oriented performance measures for the program when implemented.[11] The department implemented all three recommendations from that report.

In Senate Report 118-188, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2025, the Senate Armed Services Committee includes a provision for us to review DOD's implementation of the program.[12] Our report on the CMMC program describes (1) DOD's efforts to assist small companies in meeting related cybersecurity requirements; (2) the extent to which DOD is prepared to train its acquisition workforce on their related responsibilities; and (3) The Cyber AB's actions to prepare for the implementation of the program's requirements; and assesses (4) the extent to which DOD has a comprehensive strategy to guide implementation of the program.

For all our objectives, we reviewed policies, procedures, guidance, and prior GAO work related to DOD's implementation of the CMMC program. For our first objective, we reviewed DOD documentation and interviewed DOD officials and industry representatives (e.g., the DIB Sector Coordinating Council) who support DIB companies to describe DOD's efforts to assist small companies in meeting cybersecurity requirements related to CMMC. In support of our second objective, we reviewed DOD documentation and interviewed DOD officials who are responsible for policy, acquisition, and training to describe DOD's efforts to train the acquisition workforce for its CMMC responsibilities. For our third objective, we reviewed DOD and The Cyber AB documentation and interviewed DOD and The Cyber AB officials to describe The Cyber AB's actions to prepare for the implementation of CMMC requirements.

Regarding our fourth objective, we reviewed DOD planning documentation for the CMMC program implementation. We assessed DOD's CMMC planning documents using a scorecard methodology against seven key elements of comprehensive strategic planning that we identified in our prior work.[13] We also interviewed DOD officials and industry representatives regarding DOD's plans for the implementation of the CMMC program. For additional information on our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from December 2024 to March 2026 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

[10]GAO, *Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses*, GAO-15-777 (Washington, D.C.: Sept. 24, 2015).

[11]GAO, *Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certification Framework*, GAO-22-104679 (Washington, D.C.: Dec. 8, 2021).

[12]S. Rep. No. 118-188, at 341-42 (2024).

[13]The seven key elements of comprehensive strategic planning are: mission statement; a problem definition, scope, and methodology; goals and objectives; activities, milestones, and performance measures; resources and investments; organizational roles, responsibilities, and coordination; and key external factors that could affect goals. See GAO, *Defense Logistics: A Completed Comprehensive Strategy is Needed to Guide DOD's In-Transit Visibility Efforts*, GAO-13-201 (Washington, D.C.: Feb. 28, 2013).

audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Federal Government Cybersecurity Requirements

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. Computer systems and electronic data support virtually all federal operations, 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.

The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency reported advanced persistent threat activity that demonstrates the damage that increasingly sophisticated threats can cause and reinforces the importance of effectively protecting federal systems, including those DOD and its contractors use to achieve their missions.[14] Safeguarding federal computer systems—including those contractors operate or maintain—has been a long-standing concern. Underscoring the importance of this issue, we have included cybersecurity on our High-Risk List since 1997.[15]

The federal government has required all companies (regardless of whether they are major corporations or small businesses) that process, store, or transmit FCI while doing business with the government meet specific cybersecurity requirements. Since 2016, the federal government has required all companies to apply 15 security requirements to protect FCI, and DOD has required contractors to apply 110 security requirements to protect CUI.[16] As a federal agency, DOD follows federal acquisition regulations that require companies to meet FCI requirements and has perpetuated government-wide CUI requirements through DOD's acquisition regulation supplement. As a part of the CMMC program, DOD will require companies that use critical CUI to

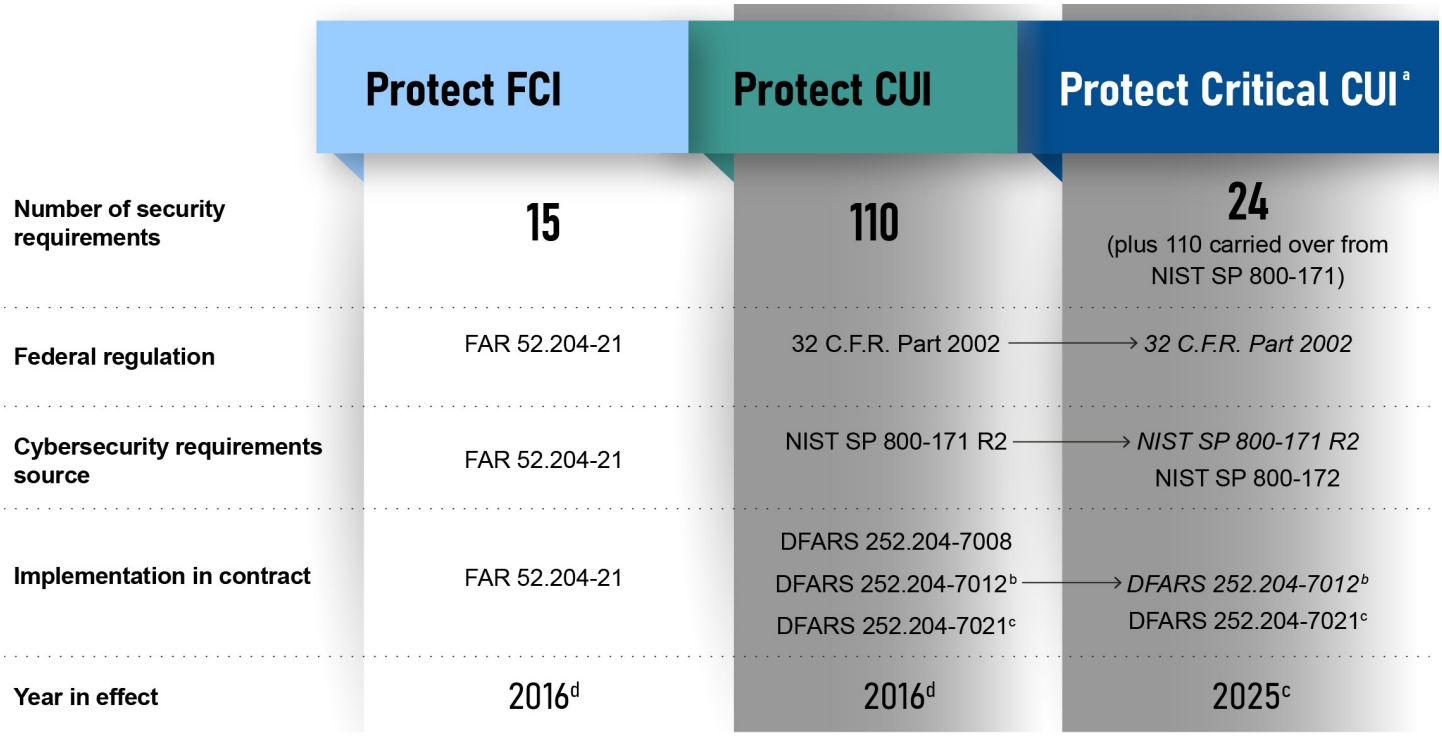
[14]Cybersecurity and Infrastructure Security Agency, Joint Cybersecurity Advisory: *Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization* (Oct. 4, 2022).

[15]GAO's High-Risk List is a biennial report that identifies government operations with vulnerabilities to fraud, waste, abuse, and mismanagement or in need of transformation. Each biennial update describes the status of high-risk areas, outlines actions that are needed to assure further progress, and identifies new high-risk areas needing attention by the executive branch and Congress. GAO, *High-Risk Series: Heightened Attention Could Save Billions More and Improve Government Efficiency and Effectiveness*, GAO-25-107743 (Washington, D.C.: Feb. 25, 2025).

[16]FAR clause 52.204-21, *Basic Safeguarding of Covered Contractor Information Systems*; DFARS clause 252.204-7012 (requiring implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171). The clauses do not apply in the case of contracts solely for the acquisition of commercial-off-the-shelf items [48 C.F.R. §§ 4.1902, 204.7304(c)].

also implement 24 of 35 additional enhanced security requirements from a related National Institute of Standards and Technology (NIST) guidance, as shown in figure 1 below.[17]

Figure 1: Cybersecurity Maturity Model Certification (CMMC) Program-Related Federal Cybersecurity Requirements and Guidance



FCI = federal contracting information, CUI = controlled unclassified information, NIST = National Institute of Standards and Technology, SP = Special Publication, C.F.R. = Code of Federal Regulation, FAR = Federal Acquisition Regulation, DFARS = Defense Federal Acquisition Regulation Supplement, R2 = Revision 2

Source: GAO analysis of Department of Defense (DOD) and National Institute of Standards and Technology (NIST) information, and federal regulations information. | GAO-26-107955

[a]NIST Special Publication 800-172 contains recommendations for enhanced security requirements to provide additional protection for CUI in nonfederal systems and organizations when such information is associated with critical programs or high value assets. The enhanced security requirements are designed to respond to the advanced persistent threat and supplement the basic and derived security requirements in NIST Special Publication 800-171. Through the CMMC program, DOD will require organizations for select contracts to implement 24 of the 35 security requirements identified in NIST Special Publication 800-172.

[b]DFARS clause 252.204-7012 requires defense industrial base contractors to report cyber incidents that affect their ability to perform requirements designated as operationally critical.

[c]DFARS clause 252.204-7021 went into effect on November 10, 2025, with the final issuance of a revision to 48 C.F.R. Part 204. DOD, *DFARS Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019–D041)*, 90 Fed. Reg. 43,560 (Sept. 10, 2025) (effective Nov. 10, 2025).

[17]Critical CUI is the term we use in this report to refer to CUI information that DOD has determined as part of the CMMC program to require enhanced security requirements from NIST Special Publication 800-172. The enhanced requirements apply to components of nonfederal systems that process, store, or transmit CUI or that provide security protection for such components when the designated CUI is associated with a critical program or high value asset. The enhanced security requirements are designed to respond to the advanced persistent threat and supplement the basic and derived security requirements in NIST Special Publication 800-171 and are intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations. See 32 C.F.R. Part 170 (2024) and NIST, NIST Special Publication 800-172: *Enhanced Security Requirements for Protecting Controlled Unclassified Information, A Supplement to NIST Special Publication 800-171* (February 2021).

[d]While the federal government did not issue any security control requirements until 2016, DOD has been working with select defense industrial base companies to protect sensitive information since 2007. See GAO, *Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats*, GAO-12-762SU (Washington, D.C.: Aug. 3, 2012).

DOD's CMMC Program History and Structure

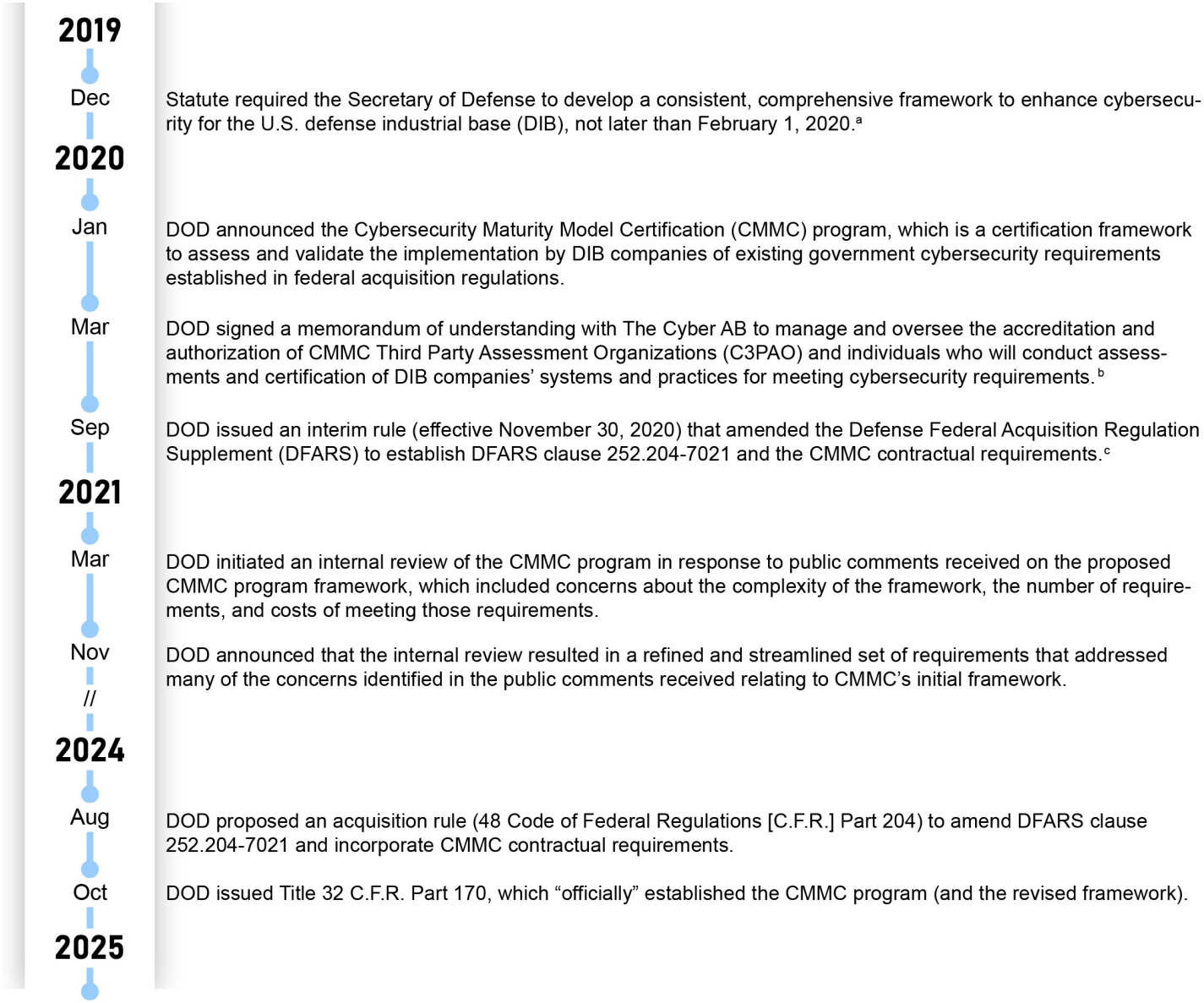
The enactment of the National Defense Authorization Act for Fiscal Year 2020 required DOD to develop a consistent, comprehensive framework to enhance cybersecurity for the DIB.[18] In response, the department began developing the CMMC program to validate that DIB companies were meeting federal government cybersecurity requirements.

DOD's initial efforts raised concerns within the DIB about the complexity of the framework, the number of requirements, and the costs of meeting those requirements. Particularly concerning were the costs for independent third-party assessments to determine if a DIB company met the requirements. Many of these concerns were held by small businesses, which represent roughly three-quarters of the DIB. In November 2021, DOD announced a refined and streamlined CMMC program framework that included estimated costs for assessments—ranging from $4,042 to $117,768 depending on the type of assessment performed—and phased implementation to allow companies time to understand the requirements and prepare. This new framework was officially established in October 2024 with the finalization of the CMMC rule in Title 32 Code of Federal Regulations (C.F.R.) Part 170.[19] DOD has taken multiple actions to implement the program as shown in the timeline below (see fig. 2).

[18]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1648 (2019).

[19]Cybersecurity Maturity Model Certification (CMMC Program), 32 C.F.R Part 170, 89 Fed. Reg. 83,092 (Oct. 15, 2024) (effective Dec. 16, 2024).

Figure 2: Timeline of DOD Efforts to Develop the CMMC Program Since 2019



Source: GAO analysis of Department of Defense (DOD) information. | GAO-26-107955

[a]National Defense Authorization Act for Fiscal Year 2020, Pub. L. No. 116-92, § 1648 (2019).

[b]DOD formalized this partnership via a no-cost contract in November 2020. Originally established as the Cybersecurity Maturity Model Certification Accreditation Body Inc. in 2020, it rebranded and has been doing business as The Cyber AB since June 2022.

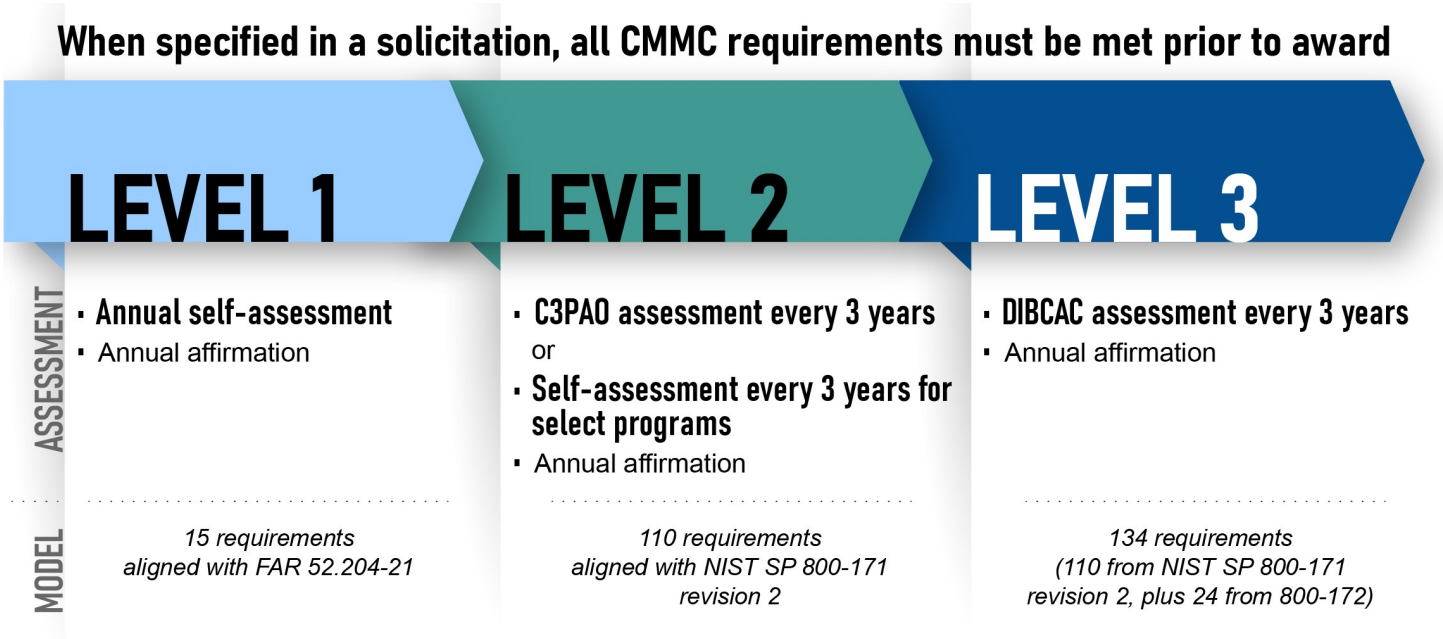
[c]DOD, *DFARS: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), Interim Rule*, 85 Fed. Reg. 61,505 (Sept. 29, 2020) (effective Nov. 30, 2020).

To establish the risk-based approach of the CMMC program, DOD organized the CMMC program to include three levels of assessment and certification requirements based on the sensitivity of the data needed to execute the requirements of the contract (see fig. 3 below). Specifically, the levels are as follows:

- Level 1 is intended for contracts that require DIB companies to handle FCI. For Level 1, DIB companies must annually conduct a self-assessment of their systems and affirm that they have implemented the 15 security requirements for protecting FCI discussed above.
- Level 2 is intended for contracts that require DIB companies to handle CUI information. Under Level 2, DIB companies that handle CUI must conduct a self-assessment of their systems every 3 years and affirm annually that they meet the 110 security requirements for protecting CUI discussed above. However, if the CUI information used by the DIB company is defense related, it cannot conduct a self-assessment but instead must undergo an assessment conducted by an accredited outside organization—known as a CMMC Third Party Assessment Organization (C3PAO)—every 3 years.[20] Upon successful completion of the assessment, the C3PAO grants the company certification status, and the company must affirm annually that they meet the requirements for protecting CUI discussed above.
- Level 3 is intended for contracts that require DIB companies to handle critical CUI information, which needs a higher level of protection than for Level 2. This level requires that the company meet the 110 Level 2 cybersecurity requirements and an additional 24 requirements for protecting critical CUI from advanced persistent threats. To achieve Level 3 certification, DIB companies must undergo an assessment of their systems conducted by DOD's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) every 3 years. Upon successful completion of the assessment, DIBCAC grants the company certification status, and the company must annually affirm that they continue to meet the requirements.

[20]For the purposes of this report, we are using the term defense-related CUI to refer to information that falls within the Defense Organizational Index Grouping of the National Archives and Records Administration's CUI Registry, to include Controlled Technical Information, DOD Critical Infrastructure Security Information, Naval Nuclear Propulsion Information, and Unclassified Controlled Nuclear Information–Defense.

Figure 3: CMMC Program Framework



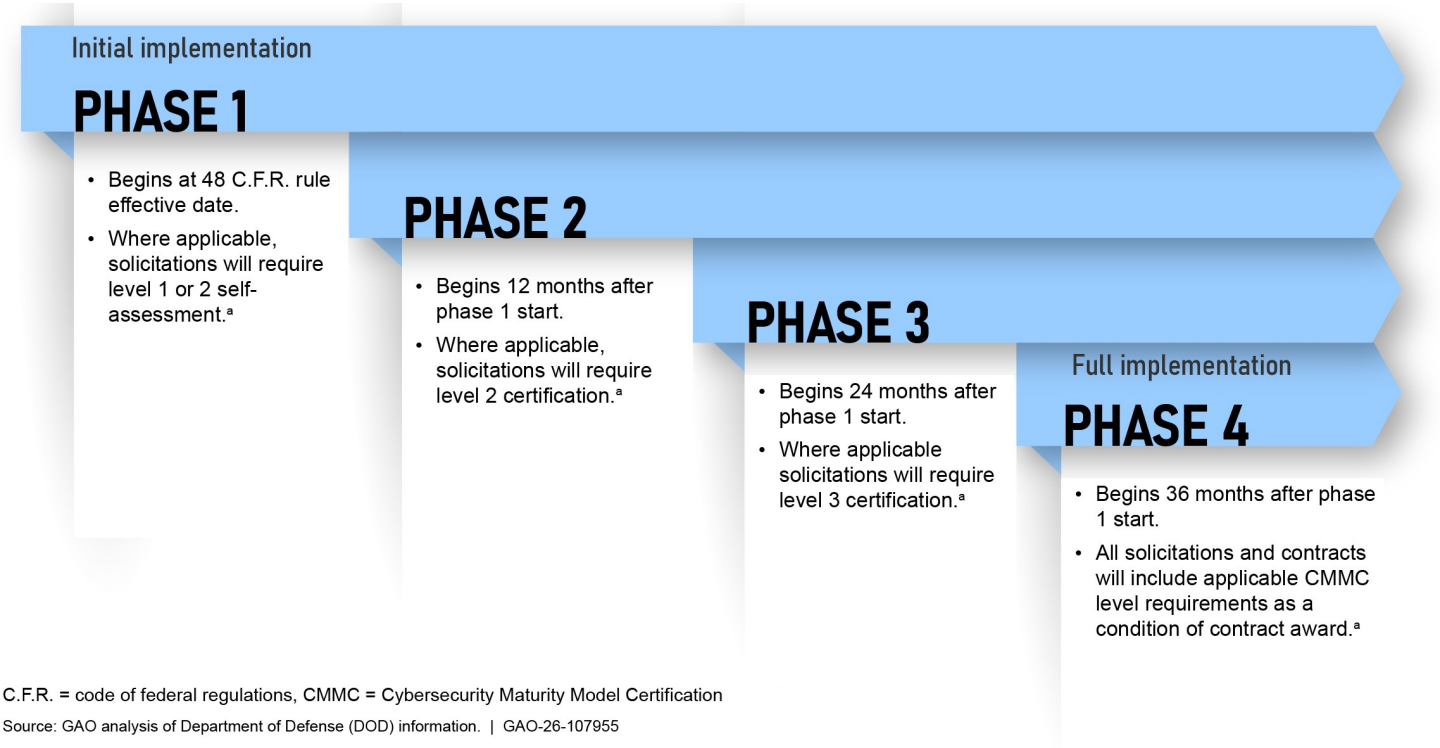
CMMC = Cybersecurity Maturity Model Certification, C3PAO = Certified Third-Party Assessment Organization, DIBCAC = Defense Industrial Base Cybersecurity Assessment Center, FAR = Federal Acquisition Regulation, NIST = National Institute of Standards and Technology, SP = Special Publication

Source: GAO analysis of Department of Defense (DOD) information. | GAO-26-107955

The program managers or requiring activities must determine the appropriate CMMC certification level requirement based on the sensitivity of the data needed to execute the requirements of contracts for products or services. Once the requiring program decides the CMMC level associated with a contract, the contracting officer is to identify that level in the contract solicitation (e.g., request for proposal). DIB companies that bid on that solicitation vehicle are required to meet the validation requirement associated with the stated CMMC level at time of award.

DOD plans to implement the CMMC program using a phased approach over a 36-month period, as shown in figure 4. The start date of the 36-month period began when the complementary 48 C.F.R. Part 204 rule, which was finalized in September 2025, went into effect on November 10, 2025. This rule incorporates CMMC contractual requirements in the Defense Federal Acquisition Regulation Supplement (DFARS).

Figure 4: CMMC Program Phased Implementation Approach



C.F.R. = code of federal regulations, CMMC = Cybersecurity Maturity Model Certification

Source: GAO analysis of Department of Defense (DOD) information. | GAO-26-107955

[a]For each phase in the CMMC implementation, DOD will apply the necessary requirements by level for assessment or certification per 32 C.F.R. Part 170. DOD may, at its discretion, include the requirement for certain phases in applicable solicitations and contracts as a condition to exercise an option period on a contract awarded prior to the effective date.

Roles and Responsibilities of DOD's CMMC-Related Organizations

The Secretary of Defense oversees DOD's effort to implement the CMMC program. Table 1 illustrates the roles and responsibilities of DOD's organizations related to the CMMC program.

Table 1: Roles and Responsibilities of CMMC Program-Related DOD Organizations

Organization	Roles and responsibilities
Cybersecurity Maturity Model Certification (CMMC) Program Management Office	Residing within the Office of the Department of Defense Chief Information Officer (CIO), Office of the Deputy CIO for Cybersecurity, the CMMC Program Management Office provides oversight of the program and is responsible for establishing assessment, accreditation, and training requirements as well as developing and updating program policies and implementing guidance.
Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)	DIBCAC resides within DOD's Defense Contract Management Agency. DIBCAC assessors conduct Level 3 certification assessments for defense industrial base (DIB) companies and issue certificates of CMMC status resulting from Level 3 certification assessments to DIB companies that have passed that assessment. DIBCAC assessors also conduct Level 2 assessments of the information systems that process, store, or transmit Controlled Unclassified Information of the accreditation body and prospective CMMC Third-Party Assessment Organizations.
Office of the Under Secretary of Defense for Acquisition and Sustainment	Principal Staff Assistant and advisor to the Secretary of Defense for all matters relating to acquisition and sustainment in the DOD to include contracting.

Organization	Roles and responsibilities
DOD programs and requiring activities	Responsible for acquisition functions within a DOD component, which includes identifying contract requirements and awarding contracts for services and products.

Source: GAO analysis of Title 32 Code of Federal Regulations Part 170 and Department of Defense (DOD) information. | GAO-26-107955

Key Elements of Comprehensive Strategic Planning

A comprehensive strategy provides the foundation upon which an agency builds its plan for defining what the agency intends to accomplish and how it will achieve desired results and meet its goals and objectives. In our prior work, we identified seven key elements that are necessary for a strategy to be comprehensive and applied them in assessing other agency strategies.[21] Table 2, below, contains descriptions of the seven key elements.

Table 2: Key Elements of a Comprehensive Strategy

Elements of a comprehensive strategy	Description of element
Mission statement	Development of a comprehensive statement that summarizes the purpose of the strategy.
Problem definition, scope, and methodology	Identification of the issues to be addressed by the strategy, the scope of the strategy, and the methodology by which it was developed and key considerations and assumptions used in the development of the strategy.
Goals and objectives	Identification of the goals and objectives to be achieved by the strategy.
Activities, milestones, and performance measures	Identification of the steps to achieve the goals and objectives, milestones, and performance measures to gauge results.
Resources and investments	Identification of costs to execute the strategy and the sources and types of resources and investments. This should include skills and technology and the human, capital, information, and other resources required to meet the goals and objectives.
Organizational roles, responsibilities, and coordination	Description of the roles and responsibilities for managing and overseeing the implementation of the strategy and the establishment of mechanisms that allow multiple stakeholders to coordinate their efforts through implementation and make necessary adjustments to the strategy based on performance.
Key external factors that could affect goals	Identification of external factors to the organization that could significantly affect the achievement of the long-term goals contained in the strategy. These external factors can include economic, demographic, social, technological, or environmental factors, as well as conditions that would affect the ability of the agency to achieve the desired results.

Source: GAO/GGD-97-180 and GAO-13-201. | GAO-26-107955

DOD Offers Resources for Small Companies in Meeting Cybersecurity Requirements

DOD organizations, including the Office of Small Business Programs, provide various resources that can assist small companies in meeting cybersecurity requirements related to CMMC. These resources range from

[21]See, for example, GAO, *Managing for Results: Critical Issues for Improving Federal Agencies' Strategic Plans*, GAO/GGD-97-180 (Washington, D.C.: Sept. 16, 1997) and GAO-13-201.

mentorship and information sharing programs to cybersecurity tools.[22] Small businesses can leverage these resources to help improve their overall security posture and to address security control requirements of the CMMC program.

DOD's Office of Small Business Programs manages DOD's Mentor-Protégé Program, which pairs up less experienced companies with advisors that are more experienced contractors.[23] According to DOD, this program helps protégé companies build capacity, among other things, by enhancing operational capabilities, project management skills, cybersecurity, and overall readiness to successfully fulfill government contracts. As of July 2025, there were 65 mentors and 65 proteges participating in the Mentor Protégé Program, according to DOD officials. The Office of Small Business Programs plans to increase the program's capacity to help small companies meet cybersecurity requirements related to CMMC through several activities, including (1) promoting the program and recruiting qualified members; (2) expanding the program to increase the involvement of nontraditional companies; and (3) enhancing the Mentor-Protégé Program portal, according to these same officials.

Additionally, the Office of Small Business Programs established a program, referred to as Project Spectrum, that is intended to increase cybersecurity awareness of small- and medium-sized companies and to help them address DOD cybersecurity contracting requirements. The program provides cybersecurity information, resources, tools, and training. As of July 2025, there are 21,535 participating companies, according to DOD officials. Project Spectrum is offered at no cost to the companies. The program's advisors are to educate companies on how to improve their cybersecurity posture and can assist them with developing the security documentation required for CMMC certification. Project Spectrum has hired additional personnel and can scale to meet the needs of small companies, according to DOD officials.

In addition, the National Security Agency's (NSA) Cybersecurity Collaboration Center offers a variety of cybersecurity services and tools at no cost to DOD contractors, including small companies, according to NSA officials. For example, NSA's Center hosts an information sharing service that is intended to provide companies with DIB-specific threat intelligence to help them prevent, detect, and mitigate malicious cyber activity. The Center also provides active defense services to detect and mitigate where a company's network might be susceptible to cybersecurity threats. These services can help a company partially address a subset of CMMC security requirements, to include those related to risk assessment. As of August 2025, there were approximately 1,600 participants across the services NSA's Center provides, according to an NSA official.

Moreover, officials we interviewed from several other DOD organizations, including the Army, Navy, Air Force, and Defense Logistics Agency Office of Small Business Programs, stated that they inform companies about the resources that are available to them to help them meet cybersecurity requirements. Additionally, industry representatives we met with stated that these resources are generally helpful for DIB companies. More information on these and additional resources are discussed in appendix II.

[22]See DOD Instruction 4205.01, *DOD Small Business Programs* (June 8, 2016) (incorporating change 1, effective Sept. 13, 2017). Mentorship programs pair less experienced individuals with more experienced professionals to provide guidance and support. Information sharing programs share information and tools to assist small companies in meeting cybersecurity requirements related to CMMC. Cybersecurity tools assist companies in implementing cybersecurity requirements related to CMMC.

[23]10 U.S.C. § 4902.

DOD Is Assessing CMMC Training and the Extent That It Will Be Required

The Defense Acquisition University (DAU) offers three voluntary CMMC-focused courses targeting different portions of the defense acquisition workforce.[24] In response to the finalized 48 C.F.R. Part 204 rule, officials in the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) told us that they are assessing these training courses to determine the extent to which (1) the content should be updated or expanded and (2) the courses should be mandatory for various portions of the acquisition workforce. The CMMC Program Management Office officials told us they see value in having much of the acquisition workforce take the DAU training.

DOD Has Developed Training Resources for the Defense Acquisition Workforce

The CMMC Program Management Office and DAU have collaborated to develop CMMC training for DOD's acquisition workforce because the program will be implemented through the department's procurement process. DAU currently offers three voluntary CMMC-related courses targeting different parts of the acquisition workforce:

- **Cybersecurity 1010.** In February 2025, DAU began offering an introductory CMMC course. This self-paced, online course provides background information, covers related DFARS clauses and provisions, and describes the certification process and participants. Further, the course addresses differences between FCI and CUI, and the various levels of certification. The course also presents the CMMC Program Management Office's plan to phase-in implementation of the program.

  DAU and OUSD(A&S) officials stated that the entire acquisition workforce had been notified of the new training and encouraged to complete it, though it primarily targets those responsible for delivering secure and resilient systems, and those who determine contract cybersecurity requirements (e.g., program and requiring activity officials). As of September 2025, 267 acquisition workforce members had completed this online training, providing DAU generally favorable reviews of its content, according to DAU officials.

- **Cybersecurity 1020.** In September 2025, DAU introduced an online, self-paced course for those responsible for drafting and implementing contracts with the DIB such as managers, contracting officers, and contracting officer's representatives. Building on material in the introductory course, this course explains the elements of the CMMC program related to the acquisition process, things to consider when determining the certification level required for a solicitation, and pre- and post-contract award requirements including the flow down of requirements to subcontractors.
- **Cybersecurity 1030.** In July 2025, DAU began offering a course for senior acquisition workforce members, such as component and service acquisition executives and program executive officers, that will provide direct support to CMMC-related decisions during a procurement. This self-paced, online course provides background on the program and its implementation and explains considerations for the acquisition workforce when selecting a certification requirement, the type of contract requirements associated with

[24]The mission of DAU is to develop a high-performing defense acquisition workforce through talent management, acquisition training, online resources, and organization support to deliver effective, affordable warfighting capabilities. Its president serves as the Chief Learning Officer of the DOD acquisition community by developing and delivering learning assets that address competencies identified by subject matter leads in particular acquisition fields.

each certification level, and the minimum requirements for flowing down certification requirements to subcontractors. The course also discusses the circumstances when a waiver for the CMMC requirement may be appropriate and the process for recording its use.[25] As of September 2025, 18 acquisition workforce members had completed this online training, providing DAU generally favorable reviews of its content, according to our analysis of completion rates and reviews.

Additional CMMC training resources. In addition to the new CMMC courses, DAU has hosted online events focused on the implementation of the CMMC program, and it maintains a number of CMMC-related resources on its public website. DAU hosted public webinars on CMMC, including one that provided an overview of the program and two others focused on the application of federal and defense regulations that underpin the CMMC Level 1 and Level 2 requirements. Videos from these webinars are accessible on the DAU Cyber Solutions website. This website also contains links to DOD's CMMC website and resources and to DAU's new courses. Finally, as part of an ongoing events series for logisticians, DAU hosted a CMMC-focused presentation in June 2025 intended to provide logisticians with a better understanding of how CMMC will support supply chain risk management.

DOD Is Assessing CMMC Training, Resources, and Requirements

Officials from DAU, OUSD(A&S), and the CMMC Program Management Office are expected to complete their assessment of existing training materials and determine who within the DOD acquisition workforce should be required to take the CMMC-related training in the first half of 2026.

For existing training materials, a DAU directive establishes standardized methods to review, process, and publish updates in an effort to help ensure effective and efficient response to regulatory changes.[26] With the issuance of the final CMMC rule on September 10, 2025, DAU is required to update its training materials to reflect the regulatory changes by January 8, 2026.[27]

Officials designated by OUSD(A&S) are required to evaluate if changes to acquisition workforce training are required following regulatory updates. These functional area leads are required by policy to certify that DAU course content and objectives for the next fiscal year (1) are current, technically accurate, and consistent with DOD policy, or (2) satisfy efforts underway to align material with recent policy or regulatory changes.[28]

[25]Program managers or requiring activities may request Service Acquisition Executives or Component Acquisition Executives approval to waive the CMMC requirement that would otherwise apply to a procurement when market research indicates that including that requirement may impede the ability to generate robust competition or delay delivery of mission critical capabilities. CMMC waivers may be requested and approved for an individual procurement or a class of procurements, and waivers will impact only whether CMMC assessments must be included in solicitation documents and resultant contracts.

[26]DAU Directive 702: *Learning Asset Review, Changes, and Publication Process* (May 13, 2024).

[27]DAU Directive 702 requires the university to incorporate revisions to training content associated with new policies within 120 days of issuance.

[28]The acquisition workforce is divided into seven functional areas: auditing, business (cost estimating and financial management), contracting, engineering and technical management, life cycle logistics, program management, and test and evaluation. Functional area leads, among other things, serve as the subject matter lead for their respective functional areas, provide USD(A&S) with functional advice and recommendations to support implementation of the Acquisition Workforce Program, coordinate with subject matter leads, and work with DAU to ensure training is available and maintained. See DOD Instruction 5000.66, *Defense Acquisition Workforce Education, Training, Experience, and Career Development Program* (July 27, 2017) (incorporating change 3, effective Mar. 25, 2022).

According to DAU's directive on updating training materials, changes in instructional priorities generated by functional area leads will be incorporated into learning assets as soon as possible.

To determine who within the DOD acquisition workforce should complete the CMMC-related training, functional area leads are required to assess training annually. Among other things, functional area leads have the authority to designate a course mandatory for a particular portion of the defense acquisition workforce. They are required to submit changes to certification training requirements to DAU at least 120 days before the release of the next fiscal year's training schedule, which in recent years has occurred in July, meaning the decisions should be made by April 2026 for the forthcoming fiscal year.

Though it does not have the authority to require changes to acquisition workforce training requirements, CMMC Program Management Office officials stated that they see value in acquisition workforce members with CMMC roles taking the new courses. It has begun discussion with OUSD(A&S) officials about the scope of the training given the complexity of the CMMC requirements and changes made from the original iteration of the program. CMMC Program Management Office representatives told us that they believe it would be beneficial if 70 percent of the targeted acquisition workforce members for each of the new DAU courses complete the training within 1 year of the CMMC program's start. Achieving that goal would require about 113,000 acquisition workforce members to take DAU's online Cybersecurity 1010 course. Officials from the CMMC Program Management Office and OUSD(A&S) have initiated a discussion about how to complete these goals, and whether courses should potentially be mandatory, with decisions expected in 2026.

The Cyber AB Administers and Facilitates the Development of the CMMC Ecosystem

The CMMC program has an external accreditation body that is responsible for administering and facilitating, on behalf of DOD, an ecosystem of private sector organizations and individuals who conduct assessments, issue certifications, and train personnel. These entities include CMMC Third Party Assessment Organizations (C3PAOs), CMMC Certified Assessors, CMMC Certified Instructors, CMMC Certified Professionals, and training organizations.[29] To fill the accreditation body role, DOD established a partnership with The Cyber AB through a Memorandum of Understanding in March 2020, and formalized it via a no-cost contract with DOD in November 2020.[30] Table 3 outlines the roles and responsibilities of the CMMC ecosystem participants.

[29]CMMC Certified Assessors, in support of a C3PAO, conduct Level 2 certification assessments of DIB companies seeking CMMC certification. CMMC Certified Instructors are subject matter experts for creating curriculum or instructors delivering training to CMMC Certified Assessors candidates. CMMC Certified Professionals provide advice, consulting, and recommendations to DIB companies seeking CMMC assessment. See 32 C.F.R. Part 170 (2024).

[30]CMMC-AB Memorandum of Understanding (Mar. 23, 2020). Originally established as the Cybersecurity Maturity Model Certification Accreditation Body Inc. in 2020, it rebranded and has been doing business as The Cyber AB since June 2022.

Table 3: Roles and Responsibilities of CMMC Program-Related Private Sector Organizations and Personnel

Organization	Roles and responsibilities
The Cyber AB	• Contracted by DOD to fulfill the responsibilities of the accreditation body for Cybersecurity Maturity Model Certification (CMMC). • Responsible for authorizing and ensuring the accreditation of C3PAOs. • Administers the CMMC ecosystem. • Publishes and enforces the CMMC Code of Professional Conduct. • Publishes the CMMC Assessment Process. • Registers CMMC Practitioners. • Adjudicates elevated appeals between C3PAOs and defense industrial base companies.
Cybersecurity Assessor and Instructor Certification Organization (CAICO)[a]	• Responsible for training, testing, authorizing, certifying, and recertifying CMMC assessors, instructors, and related professionals. • Oversees development, administration, and management pertaining to the quality of training and examination materials for CMMC assessor and instructor certification and recertification. In that role, it approves applications, manages, and supports Approved Publishing Partners, Approved Training Providers, assessors and instructors; and produces the certification examination blueprints and supports the testing providers.
CMMC Third Party Assessment Organizations (C3PAO)	• Responsible for conducting Level 2 certification assessments and issuing Certificates of CMMC Status to defense industrial base companies based on the results. • Must be accredited or authorized by The Cyber AB in accordance with the requirements set forth in 32 C.F.R. Part 170. • As part of the authorization process, C3PAOs must also undergo a Level 2 certification assessment conducted by DOD's Defense Industrial Base Cybersecurity Assessment Center and meet all requirements.
CMMC Certified Professionals (CCP)	• Complete rigorous training on CMMC and the assessment process to provide advice, consulting, and recommendations to their defense industrial base company clients. • Must obtain and maintain certification from the CAICO and are eligible to become CCAs (see below) and can participate as a CCP on Level 2 certification assessments with CCA oversight where the CCA makes all final determinations.
CMMC Certified Assessors (CCA) and Lead CCAs	• In support of a C3PAO, conduct Level 2 certification assessments of defense industrial base companies. • Must first be certified as a CMMC Certified Professional. • Must obtain and maintain certification from the CAICO. • Can qualify as a Lead CCA by having at least 5 years of cybersecurity experience, 5 years of management experience, 3 years of assessment or audit experience, and at least one foundational qualification aligned with an advanced proficiency level defined in DOD policy.
CMMC Certified Instructors (CCI)	Teach CCP, CCA, and CCI candidates and perform CMMC instructional duties. Must obtain and maintain instructor designation or certification, as appropriate, from the CAICO; and must also obtain and maintain CCP or CCA certification to deliver training, depending on the type of training they offer.
Approved Publishing Partners	Third-party companies, approved by CAICO, that develop the CMMC certification curriculum based on the objective blueprints provided by the CAICO.
Approved Training Providers	Third-party companies, approved by CAICO, that develop and deliver the CMMC certification courses and classes using approved materials developed by Approved Publishing Partners.

Source: GAO analysis of Title 32 Code of Federal Regulations Part 170 and The Cyber AB information. | GAO-26-107955

[a]Formerly a subsidiary of The Cyber AB, in December 2025, The Cyber AB announced the transfer and authorization of the CAICO role to ISACA, a professional certification association. According to officials from The Cyber AB, a transition period, during which ISACA will fully and independently assume all administrative, technical, and programmatic responsibilities of the CAICO, is planned to be completed on April 1, 2026.

The Cyber AB's actions to address these responsibilities include the following:

- **Authorizing and accrediting C3PAOs.** As of December 2025, The Cyber AB had authorized 92 C3PAOs, according to DOD officials. An additional 14 organizations have passed a CMMC Level 2 DIBCAC assessment but have not yet been authorized by The Cyber AB, and another 14 organizations are awaiting a DIBCAC assessment.
- **Managing a marketplace for CMMC professionals.** On its website, The Cyber AB hosts a marketplace for the CMMC ecosystem.[31] This website allows visitors to search for the contact information of professionals and organizations and filter by categories such as their role, the scope of services offered, and the countries that they support. As of January 2026, The Cyber AB's marketplace website lists more than 5,300 organizations and individuals in the ecosystem.
- **Conducting CMMC-related outreach to the public.** The Cyber AB conducts outreach to the public about the CMMC program through attendance at conferences and other events, and monthly virtual CMMC Town Hall meetings. According to The Cyber AB officials, they have held 61 monthly Town Halls since they began in December 2020. Additionally, according to those officials, The Cyber AB participated in 44 in-person or virtual events, including hosting two conferences of their own since 32 C.F.R. Part 170 was initially proposed in December 2023.

At the time of our review, through its subsidiary, the Cybersecurity Assessor and Instructor Certification Organization (CAICO), The Cyber AB is also responsible for training non-DOD individuals in the ecosystem.[32] CAICO's activities to address these responsibilities include the following:

- **Developing CMMC training blueprints for use by Approved Publishing Partners and Approved Training Providers.**[33] According to DOD officials, as of December 2025, CAICO had approved 11 Approved Publishing Partners and 46 Approved Training Providers.
- **Establishing quality control policies and procedures for the development of training products, instruction, and testing materials.** According to The Cyber AB officials, CAICO reviews and evaluates certification exam documentation for professionals and assessors, as well as exam item content to ensure adherence to standards, fairness, and consistency. CAICO also conducts reviews of Approved Training Providers and their instructors, and Approved Publishing Partners and their training materials to verify compliance with training requirements and quality standards.
- **Authorizing, certifying, and recertifying CMMC assessors, instructors, and related professionals.** As of December 2025, according to DOD officials, CAICO had certified 1339 CMMC Certified Professionals and 633 CMMC Certified Assessors, 290 of whom have obtained the Lead CMMC Certified Assessor designation. Also, as of August 2025, according to The Cyber AB officials, CAICO had approved 80 provisional instructors.

[31]The Cyber AB's CMMC marketplace can be found at https://cyberab.org/Catalog.

[32]In December 2025, The Cyber AB announced the transfer and authorization of the CAICO role to ISACA, a professional certification association. According to officials from The Cyber AB, a transition period, during which ISACA will fully and independently assume all administrative, technical, and programmatic responsibilities of the CAICO, is planned to be completed on April 1, 2026.

[33]Approved Publishing Partners develop the CMMC certification curriculum based on the objective blueprints CAICO provided. Approved Training Providers develop and deliver the CMMC certification courses using the approved materials that Approved Publishing Partners developed.

DOD's Plans for CMMC Met Most Key Elements of a Comprehensive Strategy

DOD's plan for the implementation of the CMMC program addresses all but one of the seven key elements of a comprehensive strategy. As previously stated, in our prior work we identified seven key elements for strategic planning that agencies should consider when developing a comprehensive plan.[34] These elements include a mission statement; goals and objectives; and organizational roles, responsibilities, and coordination; among others.

DOD does not have a strategic plan for the CMMC program recorded in a single document, but it has developed several planning documents to guide the rollout and implementation of the program. They include, for example, the regulation establishing the program (i.e., 32 C.F.R. Part 170), a regulatory impact analysis, and a CMMC implementation memorandum. We assessed the entirety of these planning documents to determine whether they considered each of the key elements for strategic planning.

We found that DOD's CMMC planning addressed six of the seven elements of comprehensive strategic planning related to defining a mission statement, a problem definition, scope, and methodology; establishing goals and objectives; defining activities, milestones, and performance measures; identifying resources and investments; and defining organizational roles, responsibilities, and coordination. However, DOD only partially addressed the element related to identifying key external factors that could impact the goals of the program (see fig. 5).

[34]See GAO-13-201.

Figure 5: Extent That DOD's Plans for the CMMC Program Rollout Addressed Key Elements of a Comprehensive Strategy, as of September 2025

Elements of a comprehensive strategy	Department of Defense (DOD) planning status	GAO assessment
Mission statement	Cybersecurity Maturity Model Certification (CMMC) program planning documentation discussed the overall purpose and included a mission statement. Specifically, 32 Code of Federal Regulations (C.F.R.) Part 170 states that the overall purpose of the CMMC program is to establish requirements for defense contractors and subcontractors to implement prescribed cybersecurity standards, establish requirements for conducting an assessment of compliance with those standards, and provide DOD with a viable means of conducting the volume of assessments necessary to verify contractor and subcontractor implementation of those cybersecurity requirements.	Addressed
Problem definition, scope, and methodology	CMMC planning documentation identified the problem to be addressed by the program and identified the scope and the methodology used to develop the program. For example, 32 C.F.R. Part 170 defines the scope of CMMC program requirements to apply to all DOD solicitations and contracts pursuant to which a defense contractor or subcontractor will process, store, or transmit Federal Contract Information or Controlled Unclassified Information on unclassified contractor information systems.	Addressed
Goals and objectives	CMMC planning documentation identified clear goals and objectives. For example, DOD has indicated that the goals of the CMMC program are to verify that the defense industrial base is safeguarding sensitive information, enforce and ensure accountability with cybersecurity standards while minimizing barriers to compliance with the requirements, and perpetuate a collaborative culture of cybersecurity and cyber resilience, and maintain public trust through high professional and ethical standards.	Addressed
Activities, milestones, and performance measures	CMMC planning documentation identified the steps to achieve the goals and objectives, and associated milestones. In addition, the documentation identified performance measures for after the program is fully implemented and provided for data collection necessary to monitor initial implementation of the program.	Addressed
Resources and investments	CMMC planning documentation identifies the types of resources and the expected personnel and technology costs to DOD and implementation costs to defense contractors for assessment or certification at each level. In doing so, the Defense Industrial Base Cybersecurity Assessment Center has identified that it does not currently have the staffing levels it requires. According to the center, it will not be able to support the expected increase in their mission workload beyond fiscal year 2027 based on current staffing levels. The center intends to request additional resources to have the staff needed to support the future needs of the CMMC program.	Addressed
Organizational roles, responsibilities, and coordination	CMMC planning documentation identifies the DOD offices' roles and responsibilities for the program and developed mechanisms for coordination between DOD and non-DOD entities (e.g., The Cyber AB and defense contractors).	Addressed
Key external factors that could affect goals	CMMC planning documentation identifies processes that can help address external factors, including a program waiver process. However, CMMC planning documentation does not systematically identify the external factors that could affect reaching each goal.	Partially addressed

Addressed: DOD documentation includes evidence that satisfies the element.

Partially addressed: DOD documentation includes evidence that satisfies some, but not all, of the element.

Not addressed: DOD documentation includes no evidence that satisfies any of the element.

Sources: GAO analysis of Department of Defense (DOD) information, and all icon illustrations. | GAO-26-107955

Specifically, DOD has not systematically identified the key factors outside of the department and beyond its control that could affect the achievement of the program's goals. DOD, The Cyber AB, CAICO, and industry officials told us that the success of the CMMC program relies extensively on external factors. Based on conversations with DOD and industry officials, we identified several external factors that could affect the success of the CMMC program. They include the following:

- **CMMC ecosystem capacity.** DOD relies on the private sector ecosystem of stakeholders (i.e., The Cyber AB, CAICO, C3PAOs, certified assessors, certified professionals) to meet the program's goals. For example, DOD relies on the industry to develop the capacity of C3PAOs and assessors needed to conduct enough assessments to meet DOD's projections.
- **Program demand.** CMMC program costs and requirements may affect the extent to which existing DIB companies decide to continue doing business with DOD. For example, small businesses may decide not to participate in the program due to the cost associated with assessment and certification.
- **Evolving cybersecurity requirements.** The CMMC program requirements are based on the cybersecurity standards set by the National Institute of Standards and Technology (NIST). In particular, some of the current CMMC program requirements are based on NIST's Special Publication 800-171 revision 2, which was issued in February 2020 and updated January 2021. However, NIST issued revision 3 of these standards in May 2024, and DOD has yet to update the CMMC program to incorporate this revision. Additionally, updating the training, procedures, and associated guidance for the program will take time. For example, according to The Cyber AB and CAICO officials, once relevant regulations and guidance have been finalized, it could take them up to a year to complete updates to training and exam materials.

DOD officials stated that they have not assessed and documented key external factors that could significantly affect the implementation of the CMMC program and developed a set of approaches to address them because these factors are outside the control of the department. Officials further indicated that they were not aware that they needed to document external factors that may affect program outcomes. CMMC Program Management Office officials told us that they believe the department can manage these risks by waiving CMMC assessment requirements (in whole or part). Specifically, in January 2025, DOD issued a memo that empowered senior DOD acquisition officials to approve waivers of CMMC assessment requirements and articulated a process for doing so.

We recognize that external factors not directly within DOD's control can affect successful implementation of the CMMC program. Planning for these factors is a key reason why applying a risk management approach would benefit the department. It would enable them to identify factors beyond their control and plan for how it will manage the program with these influences and mitigate any adverse impacts. DOD's *Risk, Issue, and Opportunity Management Guide for Acquisition Programs* identifies that programs cannot ignore external risks and should have contingency plans in place for external risks that are outside their immediate control.[35]

The waiver process cited by the CMMC Program Management Office does not necessarily address the different external factors that could adversely affect the implementation of the CMMC program. For example, the memo states that it would not be appropriate for DOD to waive CMMC requirements for a contract solicitation when requirements must be performed by cleared defense contractors.[36] Therefore, subcontractors to these companies will have to meet CMMC requirements consistent with the information shared by the cleared defense contractor even if external factors limit the capacity of the CMMC ecosystem to assess and certify them. Depending on the frequency and number of waivers DOD uses, the process could also undermine

[35]DOD, *Risk, Issue, and Opportunity (RIO) Management Guide for Defense Acquisition Programs* (September 2023) (incorporating change 2.2, effective December 2023).

[36]A cleared defense contractor is a private entity granted clearance by DOD to access, receive, or store classified information for the purpose of bidding for a contract or conducting activities in support of any program of the department. (32 C.F.R. § 236.2 (2015)).

the long-term viability of the CMMC program and its intent to verify that companies are implementing federal cybersecurity requirements.

Without identification of key external factors, DOD is increasing the risk that the program will not achieve its strategic goals. Assessing and documenting key external factors that could significantly affect the implementation of the CMMC program and developing a set of approaches to address those factors will increase the likelihood that the program will achieve its goals. This includes the safeguarding of sensitive information and enforcement of DIB compliance with existing information security standards. By documenting the key external factors and associated mitigation strategies, DOD would have a more realistic understanding of the risks facing the implementation of the CMMC program and position the department to act should challenges be found.

Conclusions

As cyber adversaries continually seek to access sensitive U.S. defense information, it becomes increasingly important for DOD to counter these persistent threats and ensure that the DIB companies it relies on safeguard its FCI and CUI information. DOD has taken steps to ensure that DIB companies comply with cybersecurity requirements by establishing the CMMC program. However, DOD's CMMC Program Management Office has not systematically identified the key external factors that may negatively affect the program. Identifying, assessing, and documenting the key external factors along with how it plans to address them, would place DOD in a better position to mitigate those risks. Accordingly, DOD would increase the likelihood that it will successfully complete the CMMC program implementation and achieve its goal of safeguarding sensitive defense information.

Recommendation for Executive Action

The Secretary of Defense should ensure the DOD Chief Information Officer assesses and documents key external factors that could significantly affect the implementation of the CMMC program and develops approaches it will take to address those factors. (Recommendation 1)

Agency Comments

We provided a draft of this report to DOD for review and comment. In written comments (reproduced in appendix III), DOD generally agreed with our findings, concurred with our recommendation, and described plans to address it.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact us at KirschbaumJ@gao.gov; DsouzaV@gao.gov; or RussellW@gao.gov. Contact points for our Offices of Congressional Relations and Media Relations may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

//SIGNED//

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

//SIGNED//

Vijay A. D'Souza
Director, Information Technology and Cybersecurity

//SIGNED//

W. William Russell
Director, Contracting and National Security Acquisitions

List of Committees

The Honorable Roger Wicker
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Mike Rogers
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Senate Report 118-188, accompanying a bill for the National Defense Authorization Act for Fiscal Year 2025, includes a provision for us to review the Department of Defense's (DOD) implementation of the revised Cybersecurity Maturity Model Certification (CMMC) program.[1] This report on the CMMC program describes (1) DOD's efforts to assist small companies in meeting related cybersecurity requirements; (2) the extent to which DOD is prepared to train its acquisition workforce on their related responsibilities; and (3) The Cyber AB's actions to prepare for the implementation of the program's requirements; and assesses (4) the extent to which DOD has a comprehensive strategy to guide the implementation of the program. For all our objectives, we reviewed documentation and interviewed DOD officials related to DOD's implementation of the CMMC program.

To understand how DOD has taken steps to support small companies in meeting cybersecurity requirements related to CMMC, we reviewed DOD documentation regarding its efforts for assisting small companies. For example, we reviewed DOD websites (e.g., the National Security Agency Cybersecurity Collaboration Center) that identify resources available to small companies. We also reviewed briefing information from the DOD Office of Small Business Programs regarding Project Spectrum to identify the tools and training offered to small companies that can be leveraged to meet cybersecurity requirements. To identify DOD-wide resources that are available to small companies to assist in meeting cybersecurity requirements, we interviewed officials from the Defense Industrial Base (DIB) Cybersecurity Program; DOD Office of Small Business Programs; and the National Security Agency Cybersecurity Collaboration Center. Further, we interviewed officials from the Army, Navy, and Air Force Offices of Small Business Programs and officials from the Office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology to identify resources specific to each military department that are available to small companies. Additionally, we interviewed nongovernment officials from the DIB Sector Coordinating Council; National Defense Information Sharing and Analysis Center; and National Defense Industrial Association to gain perspectives from nongovernment organizations that coordinate with DIB companies on the resources DOD provides to assist small companies in meeting CMMC requirements.

To determine the steps taken by DOD to prepare the acquisition workforce for implementing the CMMC program through solicitations and contracts, we reviewed federal regulations implementing the program to understand the specific actions and personnel who will be involved. We reviewed Defense Acquisition University (DAU) documentation, such as presentations and training announcements, as well as content on its website to understand what CMMC-focused courses, presentations, and other resources are available to or planned for the defense acquisition workforce. Further, we reviewed DOD instructions and DAU policies to understand how DOD ensures that its training content is adjusted to reflect policy changes and how senior acquisition officials consider changes to curriculum for acquisition workforce disciplines. Finally, we interviewed officials from the CMMC Program Management Office, the Office of the Under Secretary of Defense for Acquisition and Sustainment, and DAU to understand how CMMC training materials were developed and the extent to which new training would be mandatory.

[1]S. Rep. No. 118-188, at 341-42 (2024).

To understand the steps The Cyber AB has taken to prepare for the CMMC program's implementation, we reviewed the memorandum of understanding and no-cost contract between The Cyber AB and DOD, and the federal regulation implementing the CMMC program that define its roles and responsibilities. We collected and analyzed The Cyber AB information to determine the number of third-party assessment organizations and individuals who have qualified to conduct CMMC assessments. Through interviews with officials from the CMMC Program Management Office and The Cyber AB, we gained an understanding of the steps taken to evolve training requirements and content and perform outreach to industry.

Finally, to assess the extent to which DOD developed a comprehensive strategy to implement the CMMC program, we identified and reviewed key program documentation that describes how the department developed and intends to implement the program. Among these documents was the CMMC regulation, proposed rulemaking that will implement the program, regulatory impact analysis, and other supporting documents on DOD's planning for the implementation of the program and potential challenges DIB companies may experience during the CMMC rollout and once the program is implemented.

We assessed the content of DOD's planning and implementation documents using a scorecard methodology against seven key elements for comprehensive strategic planning that we identified in our prior work.[2] These elements are: mission statement; a problem definition, scope, and methodology; goals and objectives; activities, milestones, and performance measures; resources and investments; organizational roles, responsibilities, and coordination; and key external factors that could affect goals. Our scorecard methodology used a three-point scale to assess DOD's plans and efforts against each element. The three-point scoring system used the following three assessment scores:

- "addressed" indicates that DOD's CMMC planning documentation includes evidence that satisfies the element;
- "partially addressed" indicates that DOD's CMMC planning documentation includes evidence that satisfies some, but not all, of the element; and
- "not addressed" indicates that DOD's CMMC planning documentation includes no evidence that satisfies any of the element.

According to these criteria, for a strategy to be comprehensive, should include all seven key elements. Two analysts independently examined DOD's documents for guiding the implementation of the CMMC program and provided a preliminary score for each key element. In cases in which consensus could not be reached, a third, independent supervisory analyst then weighed the evidence and determined the final score. A program management specialist also provided a technical review of the analysis.

We conducted this performance audit from December 2024 to March 2026 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.

[2]See GAO, *Defense Logistics: A Completed Comprehensive Strategy is Needed to Guide DOD's In-Transit Visibility Efforts*, GAO-13-201 (Washington, D.C.: Feb. 28, 2013).

Appendix II: Examples of Cybersecurity-Related Resources That DOD Offers to Small Companies

Table 4: Examples of DOD Resources That Help Small Companies Meet Cybersecurity Requirements Related to the CMMC Program

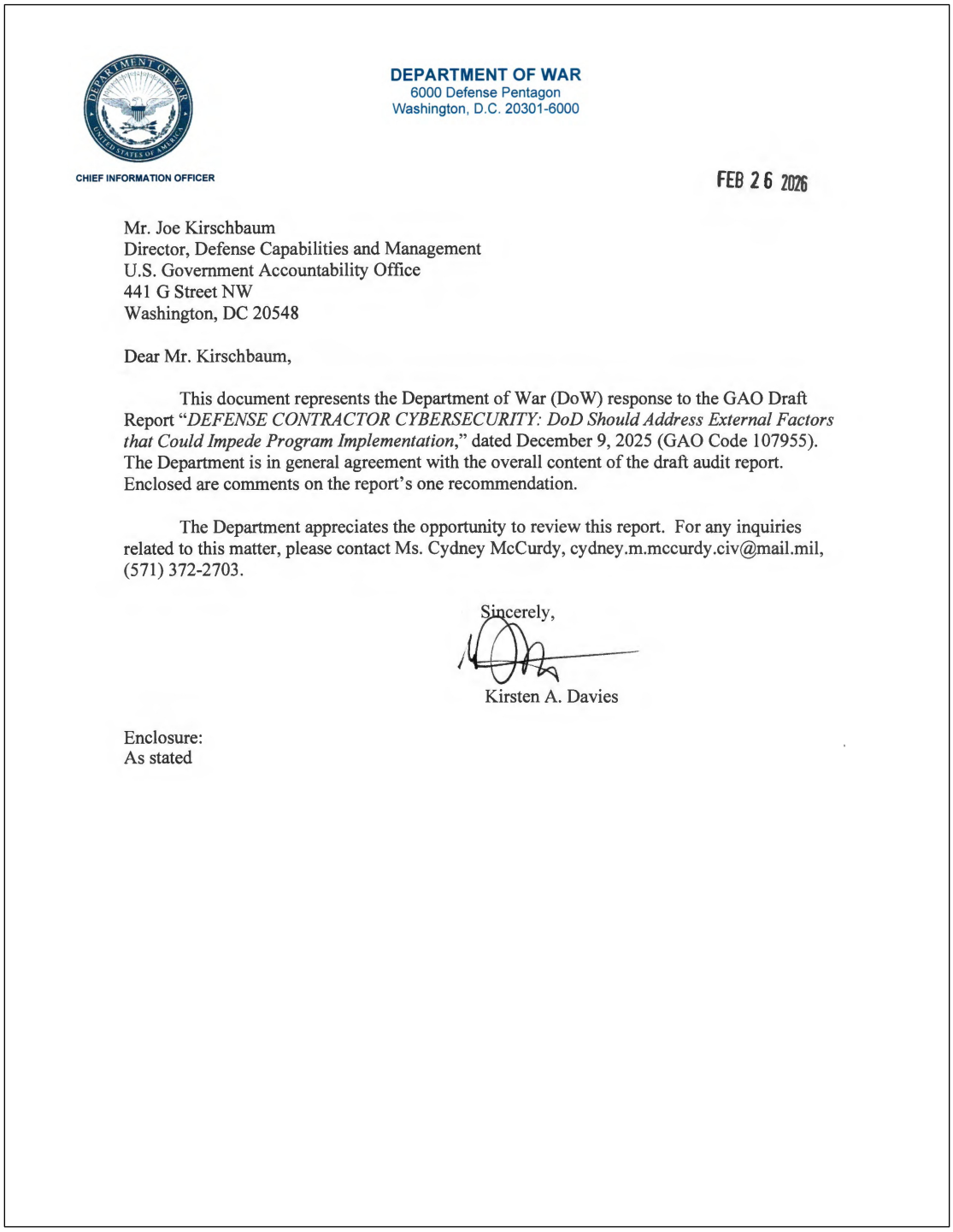
Resource type	Resource	Implementing organization	Program overview
Cybersecurity Maturity Model Certification (CMMC) program overview. These resources communicate essential details regarding the CMMC program.	CMMC 101 Brief	DOD Chief Information Officer	Provides an overview of the CMMC program including the program's history, purpose, and requirements.
	CMMC Alignment to National Institute of Standards and Technology (NIST) Standards	DOD Chief Information Officer	Provides an overview of how CMMC Level 2 is aligned with NIST SP 800-171 revision 2 standards and CMMC Level 3 is aligned with NIST 800-172 standards. Additionally, intended to provide an overview of DOD's next steps once NIST 800-172 revision 3 is finalized.
	CMMC Levels Determination	DOD Chief Information Officer	Provides an overview of the criteria for determining CMMC levels.
	CMMC Level 1 Scoping Guidance	DOD Chief Information Officer	Provides scoping guidance for companies seeking a Level 1 CMMC Certification. Including providing guidance on determining which assets will be assessed within the company's environment.
	CMMC Level 1 Assessment Guide	DOD Chief Information Officer	Provides guidance on the preparation for and execution of CMMC Level 1 self-assessment. Including, providing guidance on documenting compliance, clarifying the intent and scope of CMMC terms, the criteria, and the methodology that may be employed in a CMMC Level 1 self-assessment.
	CMMC Level 2 Scoping Guidance	DOD Chief Information Officer	Provides scoping guidance for companies seeking a Level 2 CMMC Certification. Including providing guidance on determining which assets will be assessed within the company's environment.
	CMMC Level 2 Assessment Guide	DOD Chief Information Officer	Provides guidance on the preparation for and execution of CMMC Level 2 self-assessment. Including, providing guidance regarding scope requirements, clarifying the intent and scope of CMMC terms, the criteria, and the methodology that may be employed in a CMMC Level 2 self-assessment.
	CMMC Level 3 Scoping Guidance	DOD Chief Information Officer	Provides scoping guidance for companies seeking a Level 3 CMMC Certification. Including providing guidance on determining which assets will be assessed within the company's environment.
	CMMC Level 3 Assessment Guide	DOD Chief Information Officer	Provides guidance on the preparation for and execution of CMMC Level 3 assessment. Including, providing guidance on scope requirements, clarifying the intent and scope of CMMC terms, the criteria and, the methodology that may be employed in a CMMC Level 3 self-assessment.
	Introduction to CMMC Enterprise Mission Assurance Support Service	DOD Chief Information Officer	Provides an overview of the CMMC Enterprise Mission Assurance Support Service that is used to store, track, and report on CMMC Level 2 and Level 3 assessment data.
	Supplier Performance Risk System	DOD Chief Information Officer	Provides step-by-step instruction on how to submit CMMC Level 1 and 2 self-assessments through the Supplier Performance Risk System.

Resource type	Resource	Implementing organization	Program overview
Cybersecurity services. These resources **may** assist companies in implementing **some** cybersecurity requirements related to CMMC.	Project Spectrum	DOD Office of Small Business Programs	Provides tools and training needed to increase cybersecurity awareness and maintain compliance in accordance with defense industrial base (DIB) contracting requirements, such as CMMC-related cybersecurity requirements. As of July 2025, there were 21,535 registered users for Project Spectrum, according to DOD officials.
	Valion Cloud	DOD Office of Small Business Programs	Pilot program to create a secure cloud environment that small companies can access to conduct their work while protecting sensitive information, according to DOD officials. It is not currently accessible to the public, but DOD anticipates making the program available by the end of 2025, according to DOD officials. As of July 2025, there were 75 participants using this resource, according to DOD officials.
	Next-Generation Commercial Operations in Defended Enclaves	Assistant Secretary of the Army for Acquisition, Logistics, and Technology	Pilot program to create a marketplace of providers that offer secure enclaves that small companies can access to conduct their work, according to DOD officials.[a] It is not currently accessible to the public, according to an Army official.
	Attack Surface Management	National Security Agency (NSA) Cybersecurity Collaboration Center	Intended to find and fix issues before they become compromises by inventorying and scanning parts of a company's computer or network system that are directly connected to the internet. As of August 2025, there were more than 1,300 participants using this resource, according to an NSA official.
	Continuous Autonomous Penetration Testing	NSA Cybersecurity Collaboration Center	Intended to mimic the actions of hackers to help companies find and fix potential weaknesses in their internal network system. As of August 2025, there were more than 500 participants using this resource, according to an NSA official.
	Protective Domain Name System+	NSA Cybersecurity Collaboration Center	Intended to block users from connecting to malicious or suspicious domains to drive down risk and protect DOD information. As of August 2025, there were more than 1,000 participants using this resource, according to an NSA official.
Information sharing. These resources to share information **may** assist small companies in meeting **some** cybersecurity requirements related to CMMC.	DOD Cyber Crime Center DIB Collaborative Information Sharing Environment	DIB Cybersecurity Program	Provides intelligence analysis and disseminates this information through various threat products, among other things, to enable a broad range of actions against malicious cyber activity. As of August 2025, there are approximately 1,210 participants using this resource, according to DOD officials.
	Threat Intelligence Collaboration	NSA Cybersecurity Collaboration Center	Provides companies with DIB-specific threat intelligence to help companies prevent, detect, and mitigate malicious cyber activity. As of August 2025, there were more than 1,600 participants using this resource, according to an NSA official.
Mentorship program. This resource pairs less experienced individuals with more experienced professionals to provide guidance and support.	Mentor Protégé Program	DOD Office of Small Business Programs	Partners more experienced companies with companies that are new to government contracting to provide guidance and support in becoming a part of the DIB. As of July 2025, there were 65 mentors and 65 proteges participating in this program, according to DOD officials. Additionally, the Army, Navy, and Air Force participate in the program, according to these same officials.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-26-107955

[a]An enclave is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy. *DOD Instruction 8330.01, Interoperability of Information Technology, Including National Security Systems* (Sept. 27, 2022).

Appendix III: Comments from the Department of Defense



DEPARTMENT OF WAR
6000 Defense Pentagon
Washington, D.C. 20301-6000

CHIEF INFORMATION OFFICER

FEB 26 2026

Mr. Joe Kirschbaum
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Mr. Kirschbaum,

This document represents the Department of War (DoW) response to the GAO Draft Report "*DEFENSE CONTRACTOR CYBERSECURITY: DoD Should Address External Factors that Could Impede Program Implementation*," dated December 9, 2025 (GAO Code 107955). The Department is in general agreement with the overall content of the draft audit report. Enclosed are comments on the report's one recommendation.

The Department appreciates the opportunity to review this report. For any inquiries related to this matter, please contact Ms. Cydney McCurdy, cydney.m.mccurdy.civ@mail.mil, (571) 372-2703.

Sincerely,

Kirsten A. Davies

Enclosure:
As stated

GAO DRAFT REPORT DATED DECEMBER 9, 2025
GAO-26-107955 (GAO CODE 107955)

DEFENSE CONTRACTOR CYBERSECURITY: DoD Should Address External Factors that Could Impede Program Implementation.

DEPARTMENT OF WAR COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The Secretary of Defense should ensure the DOD Chief Information Officer assesses and documents key external factors that could significantly affect the implementation of the CMMC program and develops approaches it will take to address those factors.

DoW RESPONSE: Concur. The Department will assess and document significant external factors affecting Cybersecurity Maturity Model Certification (CMMC) Program implementation, such as CMMC ecosystem capacity, program demand, and evolving cybersecurity requirements and effectiveness of CMMC requirements to address and reduce risk. The Department will also assess the fulsomeness of CMMC requirements to address the National Defense Strategy and Secretary priorities.

Accessible text for Appendix III: Comments from the Department of Defense

CHIEF INFORMATION OFFICER

Mr. Joe Kirschbaum

DEPARTMENT OF WAR

6000 Defense Pentagon

Washington, D.C. 20301-6000

Director, Defense Capabilities and Management

U.S. Government Accountability Office

441 G Street NW

Washington, DC 20548

Dear Mr. Kirschbaum,

This document represents the Department of War (DoW) response to the GAO Draft Report "DEFENSE CONTRACTOR CYBERSECURITY: DoD Should Address External Factors that Could Impede Program Implementation," dated December 9, 2025 (GAO Code 107955). The Department is in general agreement with the overall content of the draft audit report. Enclosed are comments on the report's one recommendation.

The Department appreciates the opportunity to review this report. For any inquiries related to this matter, please contact Ms. Cydney McCurdy, cydney.m.mccurdy.civ@mail.mil, (571) 372-2703.

Kirsten A. Davies

Enclosure:

As stated

GAO DRAFT REPORT DATED DECEMBER 9, 2025
GAO-26-107955 (GAO CODE 107955)

DEFENSE CONTRACTOR CYBERSECURITY: DoD Should Address
External Factors that Could Impede Program Implementation.

DEPARTMENT OF WAR COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1: The Secretary of Defense should ensure the DOD Chief Information Officer assesses and documents key external factors that could significantly affect the implementation of the CMMC program and develops approaches it will take to address those factors.

DoW RESPONSE: Concur. The Department will assess and document significant external factors affecting Cybersecurity Maturity Model Certification (CMMC) Program implementation, such as CMMC ecosystem capacity, program demand, and evolving cybersecurity requirements and effectiveness of CMMC requirements to address and reduce risk. The Department will also assess the fulsomeness of CMMC requirements to address the National Defense Strategy and Secretary priorities.

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contacts

Joseph W. Kirschbaum, KirschbaumJ@gao.gov

Vijay A. D'Souza, DsouzaV@gao.gov

W. William Russell, RussellW@gao.gov

Staff Acknowledgments

In addition to the contacts named above, Tommy Baril, Scott Borre, and Nate Tranquilli (Assistant Directors); Neil Feldman (Analyst-in-Charge); Christopher Businsky, Elisebet Lalisan, Jennifer Leotta, Lisa Maine, Terry Richardson, Tom Twambly, Theologos Voudouris, Jaya Walker, and Benjamin Wilder 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 X, LinkedIn, Instagram, and YouTube.
Subscribe to our 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

Media Relations

Sarah Kaczmarek, Managing Director, Media@gao.gov

Congressional Relations

David A. Powner, Acting Managing Director, CongRel@gao.gov

General Inquiries

https://www.gao.gov/about/contact-us