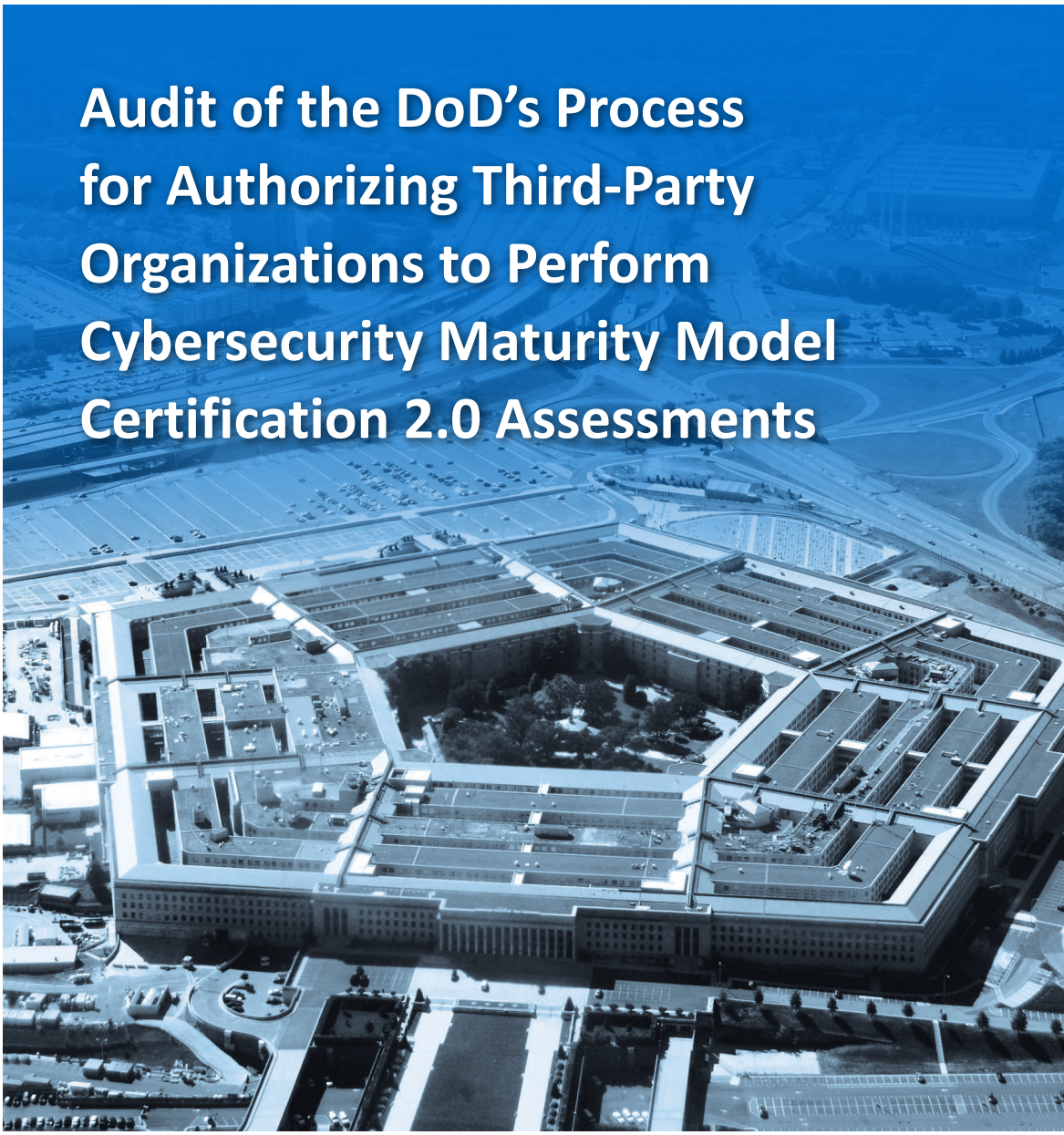
Report No. DODIG-2025-056

INSPECTOR GENERAL

U.S. Department of Defense

JANUARY 10, 2025

Audit of the DoD's Process for Authorizing Third-Party Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments



INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Results in Brief

Audit of the DoD's Process for Authorizing Third-Party Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments

January 10, 2025

Objective

The objective of this audit was to determine whether the DoD ensured that the process for authorizing third-party organizations to perform Cybersecurity Maturity Model Certification (CMMC) 2.0 assessments was effectively implemented.

Background

In November 2021, the DoD announced CMMC 2.0, a framework that requires DoD contractors to undergo cybersecurity assessments based on the criticality of the DoD information that the contractors will maintain on their systems. Contractors that will maintain controlled unclassified information critical to national security must undergo a CMMC Level 2 assessment to verify their compliance with 110 cybersecurity requirements outlined in Federal guidance. The Level 2 assessments are performed by a CMMC third-party assessment organization (C3PAO) before contract award. The C3PAOs must successfully complete a series of 12 requirements before they can be authorized to perform the Level 2 assessments. In November 2020, the DoD issued a no-cost contract to the CMMC Accreditation Body (AB) to manage the C3PAO authorization process and ensure that candidate C3PAOs meet the 12 requirements. On October 15, 2024, the DoD Chief Information Officer (CIO) published the final rule which established CMMC as a program effective on December 16, 2024.

Finding

The DoD did not ensure that the process for authorizing C3PAOs to perform CMMC Level 2 assessments was effectively implemented. Specifically, for the 11 C3PAOs that we reviewed, DoD and Cyber AB officials ensured that 10 of the 12 requirements were met before the C3PAOs were authorized to perform CMMC Level 2 assessments; however, Cyber AB officials authorized:

- two C3PAOs without ensuring that a signed C3PAO Agreement and Code of Professional Conduct was maintained for those C3PAOs;
- four C3PAOs without verifying that their quality control leads were certified; and
- all of the C3PAOs without adequately verifying that both a certified assessor and certified quality control lead were on staff or under contract as part of the assessment team.

These issues occurred because the DoD CIO did not have a quality assurance process in place for verifying that the Cyber AB authorized only those C3PAOs that met all of the requirements to perform CMMC Level 2 assessments. If the C3PAO authorization process is not effectively implemented, then the DoD does not have assurance that all C3PAOs that perform the CMMC Level 2 assessments are qualified to perform those assessments. If the C3PAOs are not qualified, then the DoD increases its risk that contractors will be awarded DoD contracts without the requirements in place to protect controlled unclassified information.

Recommendations

We made 10 recommendations to the DoD CIO, CMMC Program Management Office (PMO) Director, and Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Director, including that the DoD CIO develop and implement

Recommendations (cont'd)

a quality assurance process that will ensure that all requirements in the C3PAO authorization process are successfully met before authorizing a C3PAO to perform CMMC Level 2 assessments.

Management Comments and Our Response

The Acting DoD CIO, responding for the CMMC PMO Director, and the Defense Contract Management Agency Deputy Director, responding for the DIBCAC Director, partially agreed with the recommendations. One recommendation is closed, four recommendations are resolved but open, and five recommendations are unresolved. We request that the Acting DoD CIO, CMMC PMO Director, and the DIBCAC Director provide additional comments within 30 days of the final report for the unresolved recommendations. Please see the recommendations table on the next page for the status of recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, DoD	1	None	None
Director, Cybersecurity Maturity Model Certification Program Management Office	2.d, 2.e, 3.c	2.a, 2.c, 3.a, 3.b	2.b
Director, Defense Industrial Base Cybersecurity Assessment Center	4	None	None

Please provide Management Comments by February 10, 2025.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – The DoD OIG verified that the agreed upon corrective actions were implemented.

INSPECTOR GENERAL

DEPARTMENT OF DEFENSE

OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

January 10, 2025

MEMORANDUM FOR CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY

SUBJECT: Audit of the DoD's Process for Authorizing Third-Party Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments (Report No. DODIG-2025-056)

This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We considered management's comments on the draft report when preparing the final report. These comments are included in the report.

This report contains five recommendations that we consider unresolved because the Acting DoD Chief Information Officer (CIO) and the Defense Contract Management Agency Deputy Director did not agree with or fully address the recommendations. We will track these recommendations until the Acting DoD CIO, the Cybersecurity Maturity Model Certification (CMMC) Program Management Office (PMO) Director, and the Defense Industrial Base Cybersecurity Assessment Center Director have agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and provides adequate documentation showing that all agreed-upon actions to implement the recommendations are completed.

This report contains four recommendations that we consider resolved but open. We will close the recommendations when the CMMC PMO Director provides adequate documentation showing that all agreed-upon actions to implement the recommendations are completed.

This report contains one recommendation that we consider closed because the Acting DoD CIO took adequate action to fully address the recommendation.

DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, please provide us within 30 days your response concerning specific actions in process, completed, or alternative corrective actions proposed on the recommendations. Send your response to either followup@dodig.mil if unclassified or rfunet@dodig.smil.mil if classified SECRET.

We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [redacted].

FOR THE INSPECTOR GENERAL:

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Contents

Introduction

Objective 1

Background 1

Allegations to the DoD Hotline 7

Finding. The DoD Did Not Ensure That the Process for Authorizing Third-Party Organizations to Perform CMMC 2.0 Assessments Was Effectively Implemented 9

Cyber AB Officials Ensured That Candidate C3PAOs Met 10 of the Requirements 10

Cyber AB Officials Did Not Always Maintain Signed C3PAO Agreements and Codes of Professional Conduct 10

Cyber AB Officials Did Not Always Verify That the Quality Control Leads Were Certified 11

Cyber AB Officials' Methodology for Verifying That CCAs and Certified QCLs Were on Staff Was Inadequate 12

DIBCAC Assessors Generally Ensured That Candidate C3PAOs Implemented the Required NIST SP 800-171 Requirements 12

The DoD CIO Did Not Have a Quality Assurance Process and Plans to Rely Solely on ISO/IEC 17011 Accreditation Standards as Assurance That the C3PAO Authorization Process is Effectively Implemented 14

Other Matters of Interest: Formalizing the C3PAO Reauthorization Process 15

DoD CUI Could Be Compromised by Cyber Attacks That Weaken National Security 16

Recommendations, Management Comments, and Our Response 16

Appendixes

Appendix A. Scope and Methodology 26

Internal Control Assessment and Compliance 27

Use of Computer-Processed Data 27

Use of Technical Assistance 27

Prior Coverage 28

Contents (cont'd)

Appendix B. DoD Hotline Allegations and Results Related to the DoD's C3PAO Authorization Process and Cyber AB Accreditation Requirements 29

Appendix C. Sampling Approach 33

Appendix D. CMMC Assessor Training Track 34

Management Comments

DoD Chief Information Officer 36

Defense Contract Management Agency 40

Acronyms and Abbreviations 42

INSPECTOR GENERAL

DEPARTMENT OF DEFENSE

Introduction

Objective

The objective of this audit was to determine whether the DoD ensured that the process for authorizing third-party organizations to perform Cybersecurity Maturity Model Certification (CMMC) 2.0 assessments was effectively implemented. In addition, we reviewed three allegations from the DoD Hotline. Our conclusions related to the hotline allegations are in Appendix B. The scope, methodology, and prior coverage related to the objective are in Appendix A.

Background

In December 2019, Congress passed the FY 2020 National Defense Authorization Act, which included a requirement for the Secretary of Defense to develop a "consistent, comprehensive framework" for enhancing Defense Industrial Base (DIB) cybersecurity to protect contract and controlled unclassified information (CUI) that the DoD shares with the DIB.[1] CUI is information created or possessed by the Government that requires safeguarding or dissemination controls according to applicable laws, regulations, and government-wide policies. CUI is not classified information.

The FY 2020 National Defense Authorization Act required that the Secretary of Defense develop the framework by February 1, 2020, and include in the framework:

- unified cybersecurity standards, regulations, metrics, ratings, third-party organization certifications, or requirements to be imposed on the DIB for the purpose of assessing the cybersecurity of individual contractors;
- the roles and responsibilities of the DoD to establish and ensure DIB compliance with cybersecurity standards, regulations, and policies; and
- a plan to provide implementation guidance, education, manuals, and technical support or assistance, to contractors on matters relating to cybersecurity.

In response to the FY 2020 National Defense Authorization Act requirement, the Office of the Under Secretary of Defense for Acquisition and Sustainment developed an initial framework, referred to as CMMC 1.0, in coordination with the Offices of the DoD Chief Information Officer (OCIO) and Under Secretary of Defense for Intelligence and Security; the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC);

[1] Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," Division A, Title XVI, section 1648, Subtitle C, "Framework to Enhance Cybersecurity of the United States Defense Industrial Base," December 20, 2019. The DIB includes all organizations and facilities that provide the DoD with materials, products, and services.

universities and research centers that conduct business for the DoD; and industry.[2] In September 2020, the DoD published an interim rule to the Defense Federal Acquisition Regulation Supplement in the Federal Register (Defense Federal Acquisition Regulation Supplement Case 2019-D041), which outlined the CMMC 1.0 framework and requested comments from the public.[3]

CMMC 2.0

In November 2021, the Office of the Under Secretary of Defense for Acquisition and Sustainment announced a revised CMMC framework, referred to as CMMC 2.0, in response to the comments from the public concerning CMMC 1.0. Those comments focused on the need to reduce CMMC implementation costs and align CMMC cybersecurity requirements with existing Federal cybersecurity policy and standards. The CMMC 2.0 framework establishes a three-level system that requires contractors to undergo different levels of cybersecurity assessments based on the criticality of the DoD information that the contractors maintain on their systems. The three-level system includes contractor self-assessments, assessments performed by authorized third-party organizations, and DIBCAC-led assessments, in which the contractor is assessed on their compliance with requirements outlined in National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171 and 800-172.[4] Unlike the other assessment levels, Level 2 requires a self-assessment or a third-party organization assessment, as described in Table 1.

[2] The Defense Contract Management Agency's DIBCAC leads the DoD's contractor cybersecurity risk mitigation efforts by assessing DoD contractors' compliance with Defense Federal Acquisition Regulation Supplement clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," and National Institute of Standards and Technology Special Publication 800-171, "Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations."

[3] Defense Federal Acquisition Regulation Supplement Case 2019-D041, "Assessing Contractor Implementation of Cybersecurity Requirements," effective November 30, 2020.

[4] NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," Revision 2, February 2020 (Updated January 28, 2021). NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information," February 2021.

Table 1. CMMC 2.0 Assessment Levels

Level 1 Self-Assessment	Level 2 Self-Assessment or Third-Party Assessment	Level 3 DoD-Led Assessment
Required for DoD contractors that maintain information that requires protection but that is not critical to national security or CUI. Contractors must assess themselves on ***15 cybersecurity requirements*** that aligns with NIST SP 800-171 and complete an annual self-assessment affirming compliance with those requirements.[1]	Required for DoD contractors that maintain CUI that is not critical to national security. Contractors must assess themselves on ***110 cybersecurity requirements*** outlined in NIST SP 800-171 and complete an annual self-assessment affirming compliance with those requirements. Required for DoD contractors handling CUI that is critical to national security. Contractors must undergo an assessment performed by an authorized third-party organization on ***110 cybersecurity requirements*** outlined in NIST SP 800-171.	Required for DoD contractors that maintain CUI for the DoD's highest priority programs. Contractors must first pass all 110 cybersecurity requirements in the Level 2 assessment. Then, the contractors must undergo an assessment performed by the DIBCAC on ***24 of the 35 cybersecurity control enhancements*** outlined in NIST SP 800-172.[2]

[1] The Federal Acquisition Regulation 52.204-21, "Basic Safeguarding of Covered Contractor Information Systems," lists 15 basic cybersecurity requirements that contractors must implement on their information systems.

[2] Cybersecurity control enhancements supplement the basic and derived cybersecurity requirements outlined in NIST SP 800-171.

Source: The DoD OIG.

The DoD plans to notify prospective offerors which CMMC 2.0 level they will need to comply within the solicitation.[5] The prospective offerors will be responsible for obtaining a CMMC assessment certificate at the specified level before contract award.

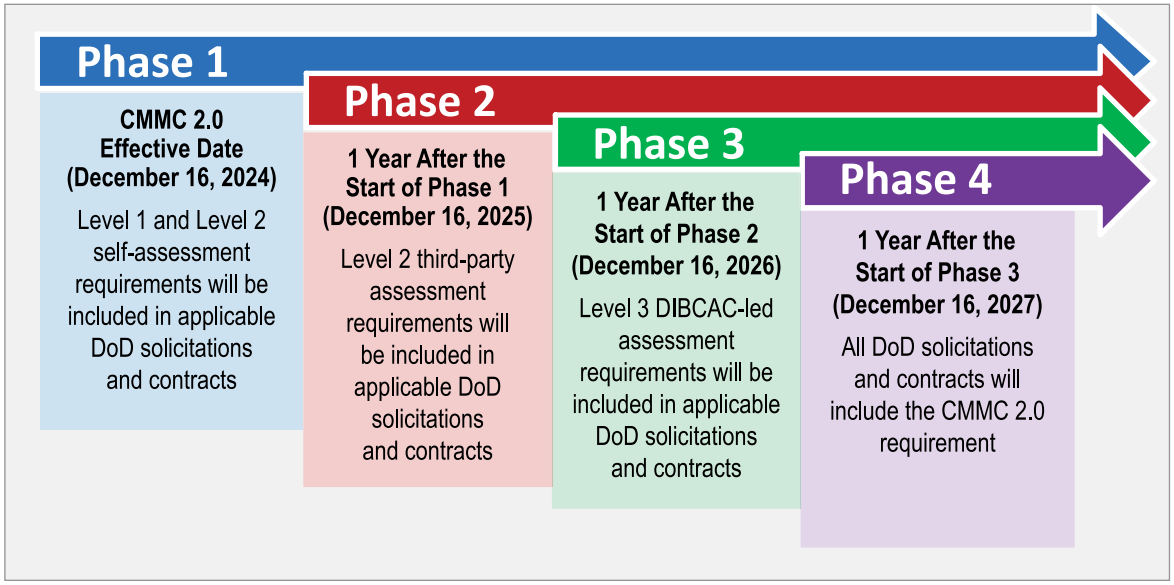
On December 26, 2023, the DoD OCIO published a proposed rule to the CMMC 2.0 framework in the Federal Register, which outlined the requirements for CMMC 2.0 and requested comments from the public.[6] The OCIO completed its review of the comments for the public and sent the comments to the Office of Management and Budget for review and comment. On October 15, 2024, the DoD OCIO published

[5] A solicitation is a request to submit offers to the Government for contracts. A prospective offeror is an entity that is actively seeking a contract.

[6] A proposed rule is an official document that announces and explains an agency's plan to address a problem or accomplish a goal.

the final rule to the Federal Register, which established CMMC as a program.[7] The final rule will become effective on December 16, 2024. According to the final rule, the DoD plans to use a four-phased approach for including the CMMC 2.0 requirement in DoD solicitations and contracts when CMMC 2.0 becomes effective on December 16, 2024, at the earliest.[8] See Figure 1 for a description of the four-phased approach.

Figure 1. Four-Phased Approach for Including the CMMC 2.0 Requirement in DoD Solicitations and Contracts if CMMC 2.0 is Effective on December 16, 2024



Source: The DoD OIG based on the phased approach described in the CMMC 2.0 Final Rule.

The DoD and Cyber Accreditation Body's Process for Authorizing Third-Party Organizations

As described in Table 1, DoD contractors that maintain CUI that is critical to national security must undergo a CMMC Level 2 assessment performed by an authorized CMMC third-party assessment organization (C3PAO).[9] Candidate C3PAOs must successfully complete a series of requirements before they can be authorized to perform the Level 2 assessments. In November 2020, the DoD issued a no-cost contract to the CMMC Accreditation Body (AB) to manage the C3PAO authorization

[7] A final rule is an official document that announces and explains an agency's requirements and the effective date of the rule. Cybersecurity Maturity Model Certification (CMMC) Program, 89 Fed. Reg. 83092-83237 (2024) (to be codified at 32 CFR part 170).

[8] The DoD will adjust the phase dates based on when the DoD must include the CMMC 2.0 requirement into DoD solicitations and contracts.

[9] A third-party organization is referred to as a C3PAO once authorized, and a candidate C3PAO while undergoing the authorization process.

process and ensure that candidate C3PAOs meet the requirements.[10] Deliverables under the contract include requirements for the Cyber AB to develop a quality control plan for its key duties; a training program for the C3PAO assessors; and monthly, quarterly, and annual status reports, among other requirements.

The candidate C3PAOs must successfully complete a series of 12 requirements before they can be authorized to perform the CMMC Level 2 assessments.[11] The Cyber AB is responsible for ensuring that the candidate C3PAOs successfully complete the following 10 requirements.

- Submit a C3PAO application to the Cyber AB.
- Pay application fee.
- Pass an organizational background check performed by the Cyber AB.
- Pass a foreign ownership, control, or influence review.
- Participate in an interview with the Cyber AB to outline the C3PAO's business operations and assessment readiness.
- Sign a C3PAO agreement and code of professional conduct.
- Pay activation fee.
- Provide verification of insurance.
- Implement an assessment appeals process that is approved by the Cyber AB.
- Employ or award a contract to a CMMC certified assessor (CCA) and a certified quality control lead (QCL).[12]

A CCA leads an assessment team, which can include other CCAs and CMMC certified professionals (CCPs); a certified QCL is responsible for observing the assessment team's conduct and assessment processes to ensure accuracy and completeness.[13] To become a CCA or certified QCL, individuals must first earn a CCP certification by demonstrating their knowledge of the CMMC framework through a series of Cybersecurity Assessor and Instructor Certification Organization-approved

[10] In June 2022, the CMMC Accreditation Body rebranded itself as the Cyber AB. The Cyber AB is a nonprofit organization that states its primary mission is to authorize and accredit the C3PAOs that perform CMMC Level 2 assessments of companies within the Defense Industrial Base. The no-cost contract between the DoD and the Cyber AB states that the duration of the contract must not exceed 10 years and 6 months.

[11] The requirements are listed on the Cyber AB website https://cyberab.org/CMMC-Ecosystem/Ecosystem-roles/Assessors-detail.

[12] A QCL is considered certified if they have certifications for both the CCA and a CMMC certified professional. The final rule does not require that C3PAOs have a certified QCL, instead it requires C3PAOs to have a quality assurance function. We refer to QCLs in the report because that was the requirement at the time we were performing the audit; however, we acknowledge the change to quality assurance function in the Management Comments section of the report.

[13] CCPs can participate on CMMC Level 2 assessments with CCA oversight; however, the CCA is responsible for the assessment results and determinations.

trainings and examinations.[14] Once individuals earn a CCP certification, they must attend additional Cybersecurity Assessor and Instructor Certification Organization-approved trainings and pass examinations to obtain certification as a CCA or QCL. The complete training track for CCAs and CCPs is in Appendix D.

The CMMC Program Management Office (PMO) and DIBCAC are responsible for ensuring that the candidate C3PAOs successfully complete the two additional requirements. The CMMC PMO Office is responsible for performing a separate organizational background check to assess the candidate C3PAO's operational risks.[15] The DIBCAC is responsible for performing a CMMC Level 2 assessment of the candidate C3PAO as the DoD requires that the candidate C3PAOs undergo the same assessment that they will be responsible for performing once they are authorized. The CMMC PMO and DIBCAC notify the Cyber AB whether the candidate C3PAOs have passed or failed the organizational background check and CMMC Level 2 assessment. Once a candidate C3PAO successfully completes all the requirements, the Cyber AB then authorizes the C3PAO to perform CMMC Level 2 assessments of prospective offerors.

CMMC Program Management Office

In February 2022, the CMMC PMO was realigned from the Office of the Under Secretary of Defense for Acquisition and Sustainment to the DoD CIO.[16] The CMMC PMO is responsible for overseeing the implementation of the CMMC program including developing and publishing the CMMC framework, the CMMC assessment guides for each CMMC level, and policies for the implementation of CMMC.[17] The CMMC PMO is also responsible for establishing requirements for CMMC assessors and assessment team members.

[14] The Cybersecurity Assessor and Instructor Certification Organization is a wholly owned subsidiary of the Cyber AB that facilitates training, examination, and professional certification for CMMC assessors and QCLs.

[15] Operational risk is the loss resulting from inadequate or failed internal processes, people, and systems or from external events.

[16] Deputy Secretary of Defense memorandum, "Elimination of the Chief Information Security Office in the Office of the Under Secretary of Defense for Acquisition and Sustainment and Assignment of Functions to Select Officials," February 2, 2022. Before the issuance of the memorandum, the Chief Information Security Office in the Office of the Under Secretary of Defense for Acquisition and Sustainment was responsible for the CMMC.

[17] CMMC assessment guides provide guidance on the assessment criteria, methodology, and findings that the certified assessors will employ during a CMMC assessment.

C3PAOs Assessed

To determine whether the DoD's process for authorizing third-party organizations to perform CMMC 2.0 assessments was effectively implemented before the authorizations were granted, we reviewed candidate C3PAO application packages and observed DIBCAC Level 2 assessments. Specifically, we:

- reviewed the application packages of a nonstatistical sample of 11 of the 48 C3PAOs that the Cyber AB had authorized to perform CMMC Level 2 assessments as of September 21, 2023,[18] and
- observed DIBCAC CMMC Level 2 assessments of a nonstatistical sample of three candidate C3PAOs.

Our detailed sampling approach for selecting the C3PAOs to review is in Appendix C.

Allegations to the DoD Hotline

After we announced the audit, we received three allegations from the DoD Hotline related to the C3PAO authorization process and the Cyber AB's compliance with its contract requirements. The allegations were submitted to the DoD OIG Hotline on May 11, 2023, September 28, 2023, and September 29, 2023. See Appendix B for additional information on our review of these complaints and our related conclusions.

Allegation 1

Allegation 1 focuses on a DIBCAC CMMC Level 2 assessment of a candidate C3PAO. Specifically, the complainant alleges that the DIBCAC did not:

- provide the candidate C3PAO with assessment guidelines before performing the Level 2 assessment;
- review all documentation provided by the candidate C3PAO that supported the implementation of certain NIST SP 800-171 cybersecurity requirements;
- provide comments supporting the DIBCAC assessor's determination that certain NIST SP 800-171 cybersecurity requirements were not implemented; and
- develop a process to appeal the results of the assessment.

[18] The Cyber AB authorized eight C3PAOs after we selected the nonstatistical sample of C3PAOs to assess.

Allegation 2

Allegation 2 focuses on the DoD's contract with the Cyber AB. Specifically, the complainant alleges that the Cyber AB did not comply with its contract requirement to obtain accreditation under the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17011.[19] The ISO/IEC 17011 accreditation standards specify requirements for the competence, consistent operation, and impartiality of accreditation bodies assessing and accrediting other organizations.

Allegation 3

Allegation 3 focuses on a DIBCAC CMMC Level 2 assessment of a candidate C3PAO. Specifically, the complainant alleges that the DIBCAC assessors requested that the candidate C3PAO provide evidence of cybersecurity requirements that are the responsibility of the candidate C3PAO's cloud service provider (CSPs) to implement.[20] The complainant states that C3PAOs cannot provide that information to the DIBCAC because, as DoD contractors, they are prohibited from downloading information concerning the CSPs cybersecurity requirements to their system.

[19] ISO/IEC 17011, "Conformity Assessment–Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies," November 2017.

[20] A CSP is an external organization that delivers services, such as data storage through the Internet.

Finding

The DoD Did Not Ensure That the Process for Authorizing Third-Party Organizations to Perform CMMC 2.0 Assessments Was Effectively Implemented

The DoD did not ensure that the process for authorizing C3PAOs to perform CMMC Level 2 assessments was effectively implemented. Specifically, for the 11 C3PAOs that we reviewed, DoD and Cyber AB officials ensured that 10 of the 12 requirements were met before the C3PAOs were authorized to perform CMMC Level 2 assessments; however, Cyber AB officials authorized:

- two C3PAOs without ensuring that a signed C3PAO Agreement and Code of Professional Conduct was maintained for those C3PAOs;
- four C3PAOs without verifying that their QCLs were certified; and
- all of the C3PAOs without adequately verifying that both a CCA and certified QCL were on staff or under contract as part of the assessment team.

In addition, of the three candidate C3PAO Level 2 assessments that we observed to determine whether the candidate C3PAO passed a CMMC Level 2 assessment, the DIBCAC assessors generally verified that the candidate C3PAOs implemented the required 110 NIST SP 800-171 requirements, except for a control related to user and group account access for two of the candidate C3PAOs.

These conditions occurred because the DoD CIO did not have a quality assurance process in place for verifying that the Cyber AB authorized only those C3PAOs that met all of the requirements to perform the CMMC Level 2 assessments.[21] Furthermore, the DoD CIO does not plan to develop a quality assurance process and, instead, plans to rely solely on the DoD's requirement that the Cyber AB comply with ISO/IEC 17011 accreditation standards as assurance that the C3PAO authorization process is effectively implemented.

If the C3PAO authorization process is not effectively implemented, then the DoD does not have assurance that all C3PAOs that perform the CMMC Level 2 assessments are qualified to perform those assessments. If the C3PAOs are not qualified to perform the Level 2 assessments, then the DoD increases its risk that contractors will be awarded DoD contracts without the requirements in place to protect CUI. Protecting CUI is critical to protecting some of the Nation's most valuable advanced defense technologies from unauthorized access and disclosure.

[21] Quality assurance is a program for the systemic monitoring and evaluation of a service to ensure that standards of quality are met.

Cyber AB Officials Ensured That Candidate C3PAOs Met 10 of the Requirements

Cyber AB officials ensured that the candidate C3PAOs met 10 of the 12 requirements before authorizing them to perform CMMC Level 2 assessments. To determine whether the C3PAOs met all of the requirements, we reviewed the C3PAO application packages for the 11 C3PAOs included in our review, interviewed CMMC PMO and Cyber AB officials, and reviewed documentation the CMMC PMO and the Cyber AB provided to support that the candidate C3PAOs met the requirement. For example, for one of the requirements, the Cyber AB performs an organizational background check of the candidate C3PAOs to ensure that they are U.S.-owned businesses and are financially stable, and to assess the candidate C3PAOs' business risks.[22] To make that determination, the Cyber AB obtained a copy of the candidate C3PAO's business credit report, which contains a financial risk assessment and any legal filings against the company. The Cyber AB evaluated each candidate C3PAO based on financial stability and operational capacity, including the candidate C3PAO's ability to pay its debts.

For one of the other requirements, the CMMC PMO performs an automated organizational background check of each of the candidate C3PAOs. The organizational background check focuses on individuals associated with the company to ensure that the individuals were not involved with any foreign adversaries, financial crimes, cybersecurity fraud, or legal filings. To make that determination, the CMMC PMO used the services of a third-party analysis company that uses artificial intelligence to interpret information from watchlists, news reports, open web sources, and proprietary lists to identify potential risks with the individuals associated with the candidate C3PAO.

Cyber AB Officials Did Not Always Maintain Signed C3PAO Agreements and Codes of Professional Conduct

Cyber AB officials did not maintain a signed C3PAO Agreement and Code of Professional Conduct for 2 of the 11 C3PAOs that we reviewed. The C3PAO Agreement and Code of Professional Conduct outline the terms, conditions, and expectations for the C3PAOs once authorized. The C3PAO Agreement requires C3PAOs to:

- pay fees for the right and privilege to provide cybersecurity assessment services;
- maintain liability insurance policies;

[22] Business risk refers to anything that could threaten a company's financial health or lead to insolvency.

- not disclose any data or information related to the Cyber AB's business or operations; and
- ensure that all personnel who perform CMMC assessments successfully complete background checks.

The Code of Professional Conduct requires C3PAOs to follow five guiding principles for professionalism, objectivity, confidentiality, proper use of methods, and information integrity.[23] Those five guiding principles are to:

- maintain a professional business posture;
- avoid the appearance of, or actual, conflicts of interests;
- maintain the confidentiality of customer and government data;
- report complete results of CMMC assessment with integrity; and
- report violations of the Code of Professional Conduct to the Cyber AB.

According to the C3PAO Agreement and Code of Professional Conduct, any breach of the Agreement or violation of the Code can result in termination of the C3PAO's authorization to perform CMMC Level 2 assessments.

The Cyber AB Chief Executive Officer stated that the C3PAO Agreement and Code of Professional Conduct for the two C3PAOs could possibly be missing because the documents did not transfer when the Cyber AB migrated to a new information technology system in June 2022. The old system was decommissioned, so the Chief Executive Officer was unable to request a search for the documentation.[24] However, without a signed copy of both documents, the Cyber AB does not have assurance that the candidate C3PAO is aware of their expectations under the documents and cannot enforce termination of the C3PAO's authorization to perform CMMC Level 2 assessments based upon a breach or violation.

Cyber AB Officials Did Not Always Verify That the Quality Control Leads Were Certified

Cyber AB officials did not verify that the QCLs for 4 of the 11 C3PAOs were certified. According to the CMMC PMO officials, individuals must obtain CCP and CCA certification before they can be designated as certified QCLs. The certification processes for the CCP and CCA are designed to provide the QCLs with training and testing on performing CMMC Level 2 assessments, and on evaluating the performance of the CCAs and the assessment team. The Cyber AB Chief Executive

[23] Proper use of methods, among other expectations, include maintaining current knowledge of and compliance with CMMC materials; not creating derivative products using Cyber AB or DoD intellectual properties; respecting the boundaries of assessment team member roles; and not unfairly influencing outcomes.

[24] Decommissioning a system removes it from service and makes the data unavailable.

Officer stated that the Cyber AB did not strictly enforce the QCL certification requirement because they did not believe that the QCLs needed technical skills to perform their responsibilities. Although the CMMC PMO officials stated that they informed the Cyber AB verbally of the requirement, the requirement was never formalized in writing.

Cyber AB Officials' Methodology for Verifying That CCAs and Certified QCLs Were on Staff Was Inadequate

Cyber AB officials authorized all 11 C3PAOs to perform Level 2 assessments without adequately verifying that the C3PAOs had both a CCA and certified QCL on staff or under contract. Specifically, the Cyber AB authorized 7 of the 11 C3PAOs without adequately verifying that a CCA was on staff, and 10 of the 11 C3PAOs without adequately verifying that a certified QCL was on staff.[25]

For the four CCAs and one certified QCL that were under contract, the Cyber AB adequately reviewed the contract terms and conditions to verify that they were responsible for leading and overseeing the CMMC Level 2 assessments for the candidate C3PAO. However, for the 7 CCAs and 10 QCLs that the candidate C3PAOs reported were on staff, the Cyber AB requested their business email address and if the address matched the candidate C3PAO's naming convention for emails, the Cyber AB considered them as valid employees. Requesting a business email address is not an adequate method for verifying employment because if the candidate C3PAO's system administrators do not delete a user's email address when they leave the company, the user would still have an active email address. In addition, ensuring that the employee has a valid user email address does not provide verification that the employee is in a position responsible for leading and overseeing CMMC Level 2 assessments.

DIBCAC Assessors Generally Ensured That Candidate C3PAOs Implemented the Required NIST SP 800-171 Requirements

For the three candidate C3PAO CMMC Level 2 assessments that we observed, the DIBCAC assessors generally verified that the candidate C3PAOs implemented the required 110 NIST SP 800-171 requirements, except for a requirement related to user and group account access for two of the candidate C3PAOs.[26]

[25] The other four CCAs and one certified QCL were under contract.

[26] A group account provides multiple users access to an organization's resources using shared authentication credentials. For example, multiple users share a password to access an application.

We accompanied DIBCAC assessors on CMMC Level 2 assessments of three candidate C3PAOs. During those assessments, the DIBCAC assessors:

- reviewed the candidate C3PAO's cybersecurity policies, plans, and procedures to determine the candidate C3PAO's processes for implementing the NIST SP 800-171 requirements;
- interviewed the candidate C3PAO's network and system administrators to gain an understanding or obtain evidence of implemented requirements; and
- identified whether the requirements were implemented as stated in the candidate C3PAO's cybersecurity policies, plans, and procedures and in accordance with NIST SP 800-171.

If the DIBCAC assessors concluded that a candidate C3PAO's process for implementing a control was in accordance with NIST SP 800-171 and the control was properly implemented, the DIBCAC assessors considered the NIST SP 800-171 requirement as "met"; if not, they considered the NIST SP 800-171 requirement as "not met." If the candidate C3PAO received at least one not met, they failed the assessment.[27]

We also reviewed the candidate C3PAO's cybersecurity policies, plans, and procedures, participated in the interviews, and observed the assessment of each requirement performed by the DIBCAC assessors. We agreed with all of the DIBCAC assessors' conclusions for one of the candidate C3PAOs and with all but one conclusion for the other two candidate C3PAOs. Specifically, we did not agree with the DIBCAC assessors' conclusions concerning the implementation of a NIST SP 800-171 requirement that requires organizations to disable or remove user and group accounts after a defined period of inactivity. Table 2 details the NIST SP 800-171 requirement, the candidate C3PAO's process for implementing the requirement, and the DIBCAC's conclusion.

Table 2. NIST SP 800-171 Requirement, Description of Implemented Requirement According to the System Security Plan, and the DIBCAC's Implementation Determination

	NIST SP 800-171 Requirement	Candidate C3PAO's Process for Implementing the Requirement	DIBCAC Determination
Candidate C3PAO One	Disable inactive user and group accounts after a defined period.	System administrators regularly monitored and disabled unused accounts.	Met
Candidate C3PAO Two	Disable inactive user and group accounts after a defined period.	User accounts disabled after 90 days of inactivity.	Met

Source: The DoD OIG.

[27] Candidate C3PAOs that fail the assessment may appeal the DIBCAC's decision.

As shown for candidate C3PAOs One and Two, the DIBCAC assessors determined that the candidate C3PAO had effectively implemented the requirement and considered the NIST SP 800-171 requirement as met. However, the DIBCAC assessors should not have considered the requirement as effectively implemented and met because:

- candidate C3PAO One's process for implementing the requirement did not define a period of inactivity after which inactive accounts would be disabled; and
- candidate C3PAO Two's process for implementing the requirement only covered user accounts and not group accounts.

According to the DIBCAC assessors, candidate C3PAO One met the intent of the requirement because the company only employed two individuals and therefore would likely not need to disable either account. However, the requirement is not contingent on the number of individuals employed at an organization and at any time, the company could expand and hire additional employees. The DIBCAC assessors stated that candidate C3PAO Two met the intent of the requirement because, according to the DIBCAC Team Chief, they historically interpreted the use of group accounts as a prohibited practice. However, neither NIST SP 800-171 nor DoD guidance prohibits organizations from using group accounts. Had the DIBCAC assessors properly applied the NIST SP 800-171 requirement, both candidate C3PAOs would have failed the Level 2 assessment.

The DoD CIO Did Not Have a Quality Assurance Process and Plans to Rely Solely on ISO/IEC 17011 Accreditation Standards as Assurance That the C3PAO Authorization Process is Effectively Implemented

The DoD CIO did not have a quality assurance process in place for verifying that the C3PAO authorization process was effectively implemented before the candidate C3PAOs are authorized by the Cyber AB to perform CMMC Level 2 assessments. Three different organizations have responsibilities associated with the C3PAO authorization process—the Cyber AB, the CMMC PMO, and DIBCAC—and the Cyber AB is also responsible for ensuring that the C3PAO successfully completes all 12 requirements before they are authorized to perform CMMC Level 2 assessments. We identified deficiencies concerning the successful completion of three of those requirements, which supports the need for a quality assurance process. However, according to CMMC PMO officials, the DoD CIO does not plan to develop a quality assurance process and instead, plans to rely solely on the DoD's requirement that the Cyber AB comply with ISO/IEC 17011 accreditation standards as assurance that the C3PAO authorization process is effectively implemented.

According to CMMC PMO officials, they consider the ISO/IEC 17011 accreditation standards sufficient to ensure that the Cyber AB is effectively implementing the C3PAO authorization process. The DoD's contract with the Cyber AB requires that the Cyber AB comply with those standards within 24 months from the effective date for CMMC 2.0. The ISO/IEC accreditation standards focus on the competency, operation consistency, and impartiality of accreditation bodies (in this case, the Cyber AB). For an organization to meet ISO/IEC accreditation standards, it must, among other things, develop policies and procedures for accrediting assessment organizations such as the C3PAOs. It must also implement a process to evaluate and monitor personnel involved in the accreditation process. While we acknowledge that ISO/IEC accreditation standards complement the Cyber AB's process to authorize the C3PAOs, it does not ensure that the Cyber AB, the CMMC PMO, and DIBCAC effectively implement that process. Furthermore, the Cyber AB has authorized and will continue to authorize C3PAOs to perform CMMC Level 2 assessments while they work toward complying with the ISO/IEC accreditation standards.

Other Matters of Interest: Formalizing the C3PAO Reauthorization Process

C3PAOs must undergo an initial CMMC Level 2 assessment and then a CMMC Level 2 reassessment every 3 years to maintain their C3PAO authorization status. Although we agree with that requirement, we do not consider it sufficient because the process does not include a review of the other requirements in the authorization process. For example, over a 3-year period, a C3PAO could experience financial problems, go under partial or full foreign ownership, lose their certified CCAs and QCLs, or change their insurance terms.

In addition to formalizing a reauthorization process, the CMMC PMO needs to establish a process for the C3PAOs to immediately self-report changes in their status with respect to any of the requirements. For example, any change to the cybersecurity requirements implemented on the C3PAO's networks and systems, or the insurance status of the C3PAO should be reported to both the CMMC PMO and Cyber AB so they are aware of the changes and can determine whether additional actions are required for the C3PAO to maintain its authorization. While the C3PAO agreements provide terms and conditions, including requiring specific insurance coverage limits, they do not provide guidance for reporting changes during the authorization period.

DoD CUI Could Be Compromised by Cyber Attacks That Weaken National Security

Because the DoD uses contractors to support their missions and often allows contractors to store DoD-specific CUI on their contractor-owned systems and networks, it is imperative for the DoD to ensure that its contractors implement the appropriate cybersecurity requirements to protect that CUI. The DoD is implementing CMMC 2.0 to enforce the protection of the CUI stored on contractor-owned systems and is relying on the C3PAOs to ensure that DoD contractors storing CUI considered critical to national security are properly implementing the 110 required NIST SP 800-171 requirements.

If the C3PAO authorization process is not effectively implemented, then the DoD does not have assurance that all C3PAOs performing CMMC Level 2 assessments are qualified to perform those assessments. If the C3PAOs are not qualified to perform the CMMC Level 2 assessments, then the DoD increases its risk that contractors will be awarded DoD contracts without the requirements in place to protect CUI. CUI, although not classified information, is sensitive information that can be critical to national security and therefore, requires safeguarding. Malicious actors have targeted DoD information maintained by DoD contractors in the past; for example, in December 2023, malicious actors blocked access to a Navy defense contractor's system, demanding money from the contractor to regain access to the system. In April 2023, malicious actors exfiltrated names and social security numbers for more than 16,000 individuals from another Navy defense contractor. Therefore, it is imperative that DoD contractors implement the required requirements to reduce the vulnerabilities that malicious actors can exploit to compromise DoD contractor systems and networks and the DoD must be able to rely on the C3PAO authorization process to ensure that the C3PAOs are qualified to perform CMMC Level 2 assessments and render an opinion on the implementation of the DoD contractor requirements.

Recommendations, Management Comments, and Our Response

Revised Recommendation

As a result of management comments, we revised Recommendation 1 to state that the DoD CIO should coordinate with the DIBCAC Director to address the recommendation.

Recommendation 1

We recommend that the DoD Chief Information Officer, in coordination with the Defense Industrial Base Cybersecurity Assessment Center Director, develop and implement a quality assurance process that will ensure that all requirements in the Cybersecurity Maturity Model Certification Third-Party Assessment Organization (C3PAO) authorization process are successfully met before a candidate C3PAO is authorized to perform Cybersecurity Maturity Model Certification Level 2 assessments.

DoD Chief Information Officer Comments

The Acting DoD CIO partially agreed, stating that the CMMC program was designed to rely on an ISO/IEC standard-compliant accreditation body to oversee the CMMC ecosystem as established in the final rule. The Acting DoD CIO also stated that they included requirements in the no-cost contract with the Cyber AB that the Cyber AB must comply with the ISO/IEC 17011 standards, which addresses quality assurance compliance and requires a peer review. The Acting DoD CIO added that the CMMC PMO maintains regular and recurring communication with the Cyber AB to discuss contract performance, including the progress of candidate C3PAOs through the authorization process, and that the Office of the DoD CIO conducts contractual oversight of the no-cost contract with the Cyber AB.

Our Response

Comments from the Acting DoD CIO partially addressed the recommendation; therefore, the recommendation is unresolved. We acknowledge in this report that ISO/IEC 17011 accreditation standards complement the Cyber AB's process to authorize the C3PAOs. However, the Cyber AB is not the only organization that has responsibilities associated with the C3PAO authorization process. The CMMC PMO is responsible for conducting background investigations, and the DIBCAC is responsible for conducting the CMMC Level 2 assessments of the candidate C3PAOs, both key steps in the authorization process. Although the Acting DoD CIO states that their office conducts contract oversight of the no-cost contract with the Cyber AB, we were unable to verify that oversight was being conducted. The contract states that the Office of the DoD CIO will hold meetings with the Cyber AB, be provided authorization records and status, and be provided results of all ISO/IEC 17011 peer reviews, but according to the CMMC PMO they do not review the authorization records for accuracy and completeness. Furthermore, the Cyber AB is not required to comply with ISO/IEC 17011 accreditation standards until 24 months from the CMMC 2.0 effective date, which is December 2026, at the earliest.

On November 7, 2024, the DIBCAC Deputy Director informed the audit team that the DIBCAC was developing a quality assurance plan that would apply to the C3PAO CMMC Level 2 assessments that the DIBCAC conducts. The Deputy Director stated that their goal is to establish a position, separate from the quality assurance official assigned to each assessment team, that will review or observe a sample of assessments in real time and perform quality assurance over the DIBCAC assessors performing the C3PAO CMMC Level 2 assessments. Because of the DIBCAC Deputy Director's plans to have an independent quality assurance official review or observe a sample of CMMC Level 2 assessments, and because the Level 2 assessment is a key step in the C3PAO authorization process, we revised this recommendation to state that the DoD CIO should coordinate with the DIBCAC Director to develop and implement a quality assurance process for the entire authorization process.

Therefore, we request that the Acting DoD CIO provide additional comments, within 30 days of the final report, describing how they will ensure that all requirements in the C3PAO authorization process are successfully met before a candidate C3PAO is authorized to perform CMMC Level 2 assessments.

Recommendation 2

We recommend that the Cybersecurity Maturity Model Certification (CMMC) Program Management Office Director direct the contracting officer to modify the contract with the Cyber Accreditation Body to require the Cyber Accreditation Body (Cyber AB) to:

a. Verify that the Cyber AB has signed Cybersecurity Maturity Model Certification Third-Party Assessment Organization (C3PAO) Agreements and Codes of Professional Conduct for every authorized C3PAO within 30 days of the date of this report or revoke the C3PAO's authorization to perform CMMC Level 2 assessments until the documents are received.

Cybersecurity Maturity Model Certification Program Management Office Comments

The Acting DoD CIO, responding for the CMMC PMO Director, partially agreed, stating that the CMMC PMO received confirmation from the Cyber AB that all currently authorized C3PAOs have provided the required C3PAO Agreements and Code of Professional Conduct, and that the Cyber AB will retain the associated documentation on file. The Acting DoD CIO also stated that the CMMC PMO Director requested that the Cyber AB implement a process to report the documentation status of each C3PAO in advance of any future authorizations and will pursue a contract modification to clarify the reporting requirement and to align the contract with the final rule.

Our Response

Comments from the Acting DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CMMC PMO Director provides a copy of the C3PAO Agreement and Code of Professional Conduct for each of the authorized C3PAOs.

b. Develop a formalized quality control lead certification requirement.

Cybersecurity Maturity Model Certification Program Management Office Comments

The Acting DoD CIO, responding for the CMMC PMO Director, partially agreed, stating that the requirement that QCLs be certified is not necessary because the requirement is not defined in the CMMC program and that instituting such a requirement would require significant revisions to the final rule. The Acting DoD CIO added that the final rule requires the C3PAOs to implement a quality assurance function that will ensure that the C3PAO assessment reports are completed accurately and in accordance with all assessment guidelines and requirements before submission to the DoD. The Acting DoD CIO also stated that the individual performing the quality assurance function:

- must be a CCA to ensure they have the appropriate technical qualifications and assessment experience; and
- cannot serve as a member of an assessment team for which they are reviewing for quality assurance to prevent conflicts of interest.

Our Response

Although the Acting DoD CIO partially agreed, the requirement in the final rule that the C3PAOs implement a quality assurance function and that the individual performing the quality assurance must be a CCA and independent of the assessment team, meets the intent of the recommendation. We reviewed the final rule; therefore, the recommendation is closed.

c. Verify that the quality control leads (QCL) for every authorized Cybersecurity Maturity Model Certification Third-Party Assessment Organization (C3PAO) meet the certification requirement within 30 days of the date of this report, and, for any of the C3PAO's QCLs who are not certified, revoke the authorization for those C3PAOs to perform CMMC Level 2 assessments until the C3PAOs provide support the QCLs are certified.

Cybersecurity Maturity Model Certification Program Management Office Comments

The Acting DoD CIO, responding for the CMMC PMO Director, partially agreed, stating that the final rule and the DoD contract with the Cyber AB subject C3PAOs to quality assurance reviews and require that the Cyber AB ensure that C3PAOs implement a quality assurance function. The Acting DoD CIO stated that the CMMC PMO Director will pursue a contract modification to clarify the quality assurance function.

Our Response

In November 2024, the CMMC PMO Director informed the audit team that all of the C3PAOs must be reauthorized before they can begin performing CMMC 2.0 assessments. The CMMC PMO stated that the reauthorization will include verification that the individual performing the quality assurance function is a CCA and that they have the appropriate technical qualifications and assessment experience. That action meets the intent of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CMMC PMO Director provides documentation verifying that the reauthorizations are completed and that they included verification that the C3PAO implemented a quality assurance function.

d. Verify the employment status of the on-staff CMMC certified assessors and certified quality control leads (QCL) by requesting and reviewing employment records to confirm that CMMC certified assessors and certified QCLs are part of the candidate Cybersecurity Maturity Model Certification Third-Party Assessment Organization's staff and are assigned those specific roles and responsibilities.

e. Verify the employment status of the CMMC certified assessors and certified quality control leads of all previously authorized Cybersecurity Maturity Model Certification Third-Party Assessment Organizations (C3PAOs) using the methodology defined in Recommendation 2.d within 30 days of the date of this report and revoke the C3PAO's authorization to perform CMMC Level 2 assessments if the employment status cannot be verified.

Cybersecurity Maturity Model Certification Program Management Office Comments

The Acting DoD CIO, responding for the CMMC PMO Director, partially agreed, stating that the DoD cannot mandate that individuals assigned to quality assurance functions, or any other staff, be employed as a permanent member of the C3PAO because the DoD is limited by the CMMC roles and responsibilities published

in the final rule and the forces of an open market CMMC ecosystem. The Acting DoD CIO stated that the final rule specifies that the DoD assign the responsibility to manage and track assessor certification status to the Cybersecurity Assessor and Instructor Certification Organization, who ensures that the certification status of the assessors is provided to the C3PAOs. The Acting DoD CIO also stated that the final rule assigned responsibility to the Cyber AB for ensuring that C3PAOs comply with the requirement to use certified assessors and that the individuals performing the quality assurance function are CCAs and not members of the team that completed the quality assurance review and report. The Acting DoD CIO stated that the assessor certification and C3PAO requirements specified in the final rule are managed in accordance with ISO/IEC 17024 and ISO/IEC 17020 standards, respectively.[28] The Acting DoD CIO stated that verification of C3PAO staff employment status by the CMMC PMO is governed by the contract with the Cyber AB and the C3PAO.

Our Response

Comments from the Acting DoD CIO did not address the specifics of the recommendations; therefore, the recommendations are unresolved. The recommendations were based on our finding that the methodology used by the Cyber AB to verify the employment status of a candidate C3PAO's CCAs and quality assurance individuals was inadequate. As stated in this report, the methodology used by the Cyber AB to verify employment was to request the employee's business email address and if the address matched the candidate C3PAO's naming convention for emails, the Cyber AB considered them as valid employees. However, requesting a business email address is not an adequate method for verifying employment because if the candidate C3PAO's system administrators do not delete a user's email address when they leave the company, the user would still have an active email address. In addition, ensuring that the employee has a valid user email address does not provide verification that the employee is actually assigned to a position responsible for leading and overseeing the CMMC Level 2 assessments for the candidate C3PAO.

Therefore, we request that the CMMC PMO Director provide additional comments, within 30 days of the final report, describing how they will modify the Cyber AB contract to require them to verify the employment status of the candidate C3PAO's CCA and quality assurance individuals by reviewing the candidate C3PAO's employment records and the action taken for any authorized C3PAOs that the employment status cannot be verified.

[28] ISO/IEC 17024, "Conformity assessment–General requirements for bodies operating certification of persons," July 2012. ISO/IEC 17020, "Conformity assessment–Requirements for the operation of various types of bodies performing inspection," March 2012.

Recommendation 3

We recommend that the Cybersecurity Maturity Model Certification (CMMC) Program Management Office Director:

a. Develop and implement a formal reauthorization process for the Cybersecurity Maturity Model Certification Third-Party Assessment Organizations (C3PAO) that includes a review and verification for all requirements in the C3PAO authorization process.

Cybersecurity Maturity Model Certification Program Management Office Comments

The Acting DoD CIO, responding for the CMMC PMO Director, partially agreed, stating that the initial C3PAO authorization and reauthorization processes are the same. The Acting DoD CIO also stated that the CMMC PMO Director will pursue the addition of a new contract deliverable that will outline the Cyber AB's internal processes for tracking and managing the authorization and reauthorization of C3PAOs.

Our Response

Comments from the Acting DoD CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved but open. We will close the recommendation once the CMMC PMO Director provides documentation that defines that the triennial reauthorization process includes all requirements of the initial authorization process. We acknowledge that adding a contract deliverable that will outline the Cyber AB's internal processes for tracking and managing the authorization and reauthorization of C3PAOs will help ensure that the reauthorizations are conducted in a timely manner.

b. Develop and implement a process to ensure Cybersecurity Maturity Model Certification Third-Party Assessment Organizations (C3PAO) immediately notify both the CMMC Program Management Office and Cyber Accreditation Body of any changes associated with any of the requirements in the C3PAO authorization process.

Cybersecurity Maturity Model Certification Program Management Office Comments

The Acting DoD CIO, responding for the CMMC PMO Director, partially agreed, stating that the Cyber AB oversees a C3PAO's status, which requires the C3PAO to report changes associated with any of the requirements in the C3PAO authorization process to the Cyber AB. The Acting DoD CIO stated that the CMMC PMO Director plans to modify the Cyber AB contract to direct the Cyber AB to revise its

procedures to ensure that C3PAOs notify the Cyber AB of any changes associated with C3PAO requirements for authorization, reauthorization, or accreditation in a timely manner. The Acting DoD CIO also stated that the CMMC PMO plans to add new contract deliverables that will require the DoD to be notified of C3PAO reporting.

Our Response

Although the Acting DoD CIO partially agreed, the planned actions to modify the Cyber AB contract to require timely notification of changes associated with C3PAO authorization requirements and to add a contract deliverable requiring the Cyber AB to notify the DoD of those changes meet the intent of the recommendation. Therefore, the recommendation is resolved but open. We will close the recommendation once the CMMC PMO Director provides a copy of the modified contract that requires the C3PAO and Cyber AB to report any changes in C3PAO authorization requirements.

c. Revise the CMMC assessment guides to further define the requirement for disabling inactive accounts to include group accounts.

Cybersecurity Maturity Model Certification Program Management Office Comments

The Acting DoD CIO, responding for the CMMC PMO Director, partially agreed, stating that there is no need for additional action as the requirement is in NIST SP 800-171, which states that disabling "identifiers," include a specific entity, object, or group. The Acting DoD CIO stated that the CMMC assessment guides align with the meaning of the NIST guidance.

Our Response

Comments from the Acting DoD CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. We agree that the CMMC assessment guides align with the NIST SP 800-171 requirement to disable or remove user and group accounts after a defined period of inactivity. However, the DIBCAC assessors did not consistently define or apply the requirement when conducting the CMMC Level 2 assessments. As stated in this report, DIBCAC assessors incorrectly determined that an assessment of the user and group accounts was not necessary for one of the candidate C3PAOs and incorrectly determined that the use of group accounts was a prohibited practice and did not need to be assessed for one of the other candidate C3PAOs. Further defining the requirement for disabling inactive accounts, including group accounts, should reduce the risk that the DIBCAC assessors conclude that a candidate C3PAO met the NIST SP 800-171 requirement when it did not.

Therefore, we request that the CMMC PMO Director provide additional comments, within 30 days of the final report, describing the plan to revise the CMMC assessment guides to further define the requirement for disabling inactive accounts, including group accounts.

Recommendation 4

We recommend that the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Director require the DIBCAC assessors to retest the requirement for disabling user and group accounts after a defined period of inactivity for every Cybersecurity Maturity Model Certification Third-Party Assessment Organization previously authorized to perform Level 2 assessments.

Defense Industrial Base Cybersecurity Assessment Center Comments

The Defense Contract Management Agency Deputy Director, responding for the DIBCAC Director, partially agreed, stating that the DIBCAC will review 25 percent of the C3PAO CMMC Level 2 assessments conducted in the last 2 years and will take appropriate action based on the results of the review by December 13, 2024. The Deputy Director agreed that candidate C3PAO One did not define a period of inactivity after which inactive accounts would be disabled, and that requirement should have been scored as "Not Met." However, the Deputy Director disagreed that candidate C3PAO Two should have been scored as "Not Met" because the candidate C3PAO's cloud environment does not allow group accounts; therefore, they did not need a process for disabling group accounts. The Deputy Director stated that no group accounts were observed by the Defense Contract Management Agency or the DoD OIG audit team during the assessment of candidate C3PAO Two.

The Deputy Director stated that the DIBCAC Director will send an email to the entire organization on testing the requirement for disabling user and group accounts after a defined period of inactivity and provide follow-on training during the DIBCAC's biweekly training session. The Deputy Director also stated that the training team will evaluate its existing assessor training course to reiterate that identifiers include specific entities (user, non-person entity), objects (computers, printers, and other devices), or groups (distribution groups), regardless of whether they are identified in the system security plan or observed during the assessment. The Deputy Director stated that these actions will be completed by October 18, 2024.

Our Response

Comments from the Defense Contract Management Agency Deputy Director partially addressed the recommendation; therefore, the recommendation is unresolved. The DIBCAC Deputy Director's plans for retesting the requirement for disabling user and group accounts after a defined period of inactivity for 25 percent of the C3PAO CMMC Level 2 assessments conducted in the last 2 years is not sufficient. Because the DIBCAC assessors did not consistently define or apply the requirement to disable or remove user and group accounts after a defined period of inactivity, and we identified at least one C3PAO that should have failed the Level 2 assessment because of that inconsistency, DIBCAC should assess all the previously authorized C3PAOs. Therefore, we request that the DIBCAC Director provide additional comments, within 30 days of the final report, describing DIBCAC's plan to retest the requirement for disabling user and group accounts after a defined period of inactivity for all previously authorized C3PAOs.

The information provided by the Defense Contract Management Agency Deputy Director about candidate C3PAO Two's cloud environment was not shared with us during the audit. Specifically, the Deputy Director stated that, while the creation of group accounts (an account with shared credentials) is possible in a cloud environment, doing so would violate the terms of service (license by user seats) established by the cloud service provider. However, the Deputy Director did not provide supporting documentation that would allow us to verify that establishing group accounts is not allowed. Therefore, we did not revise finding language on pages 9 and 14 of this report. We request that the DIBCAC Director provide documentation, within 30 days of the final report, such as a copy of the terms of services that explicitly prohibits the creation of group accounts.

We also acknowledge the additional actions that the Deputy Director plans to take with respect to notifying DIBCAC personnel on user and group account testing and providing follow-on training will further ensure that the user and group account testing considers all entities, objects, and groups, regardless of whether they are identified in the system security plan or observed during the assessment.

Appendix A

Scope and Methodology

We performed this performance audit from September 2023 through September 2024 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.

To understand the controls in place to ensure that the DoD effectively implemented the C3PAO authorization process, we reviewed the DoD's no-cost contract with the Cyber AB. Based on the responsibilities outlined in the contract, we interviewed officials from the:

- CMMC PMO;
- DIBCAC; and
- Cyber AB.

We interviewed chief executive officers, directors, and information technology specialists to identify the C3PAO authorization process. We also interviewed DIBCAC assessors to identify the cybersecurity requirements required to protect CUI.

We selected a nonstatistical sample of 11 of 48 authorized C3PAOs from the Cyber AB Marketplace as of September 21, 2023.[29] We reviewed the application packages of those C3PAOs to assess whether controls were in place to ensure that the C3PAOs met all requirements before the Cyber AB authorized them to perform CMMC Level 2 assessments. We also selected a nonstatistical sample of three out of four candidate C3PAOs that underwent a CMMC Level 2 assessment during our audit to observe DIBCAC assessors perform the Level 2 assessments as part of the authorization process.

In addition, we attended the DIBCAC's assessor training to understand how the DIBCAC assessors perform CMMC Level 2 assessments on candidate C3PAOs. We also observed DIBCAC assessors perform Level 2 assessments on three candidate C3PAOs to gain an understanding of how the DIBCAC assessors determined that the required cybersecurity requirements were met. See Appendix C for our sampling approach.

[29] The Cyber AB Marketplace is an online repository that centralizes information, including authorized C3PAOs, CCAs, and CCPs, for interested parties and service providers involved in the CMMC framework.

The Cyber AB was provided the opportunity to review and comment on relevant portions of the draft report. The Cyber AB did not provide any comments to consider in preparing the final report.

Internal Control Assessment and Compliance

We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the internal controls environment related to the DoD's process for authorizing C3PAOs to perform CMMC Level 2 assessments to ensure that the process was effectively implemented before the authorizations were granted. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Use of Computer-Processed Data

We used computer-processed data maintained by the Cyber AB to develop a universe of individuals the Cyber AB recognized as CCAs and QCLs. Specifically, we used a manually developed Microsoft Excel spreadsheet of the names of the authorized C3PAOs we selected, with their respective CCAs and QCLs. To assess the reliability of the data, we compared the spreadsheet to the names listed on the Cyber AB Marketplace and the Provisional Assessor Roster.[30] We were able to verify that the names listed on the spreadsheet were contained on the Cyber AB Marketplace or the Provisional Assessor Roster. Therefore, the list was sufficiently reliable to determine whether individuals were recognized as CCAs and QCLs.

Use of Technical Assistance

The Operations Research Analyst in our Quantitative Methods Division reviewed audit documents and advised us on the nonstatistical sampling methodology that we used to select 11 of 48 authorized C3PAOs to review. See Appendix C for our sampling approach.

[30] The Provisional Assessor Roster is a list of assessors the Cyber AB temporarily authorized to perform formal assessments and provide feedback to the Cyber AB to improve the assessment guide and methodology.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) issued one report discussing the DoD's implementation of the CMMC framework. Unrestricted GAO reports can be accessed at http://www.gao.gov.

GAO

Report No. GAO-22-104679, "Defense Contractor Cybersecurity: Stakeholder Communication and Performance Goals Could Improve Certification Framework," December 8, 2021

> The GAO found that the DoD did not provide sufficient details and timely communication on CMMC implementation. In addition, although the DoD planned to pilot the CMMC framework, the GAO found that the DoD's pilot program did not align with GAO's best practices for an effective pilot design. Specifically, the DoD did not define when and how it will analyze data from the pilot to measure performance of the CMMC framework. The DoD also did not develop outcome-oriented measures to assess the effectiveness of the CMMC.

Appendix B

DoD Hotline Allegations and Results Related to the DoD's C3PAO Authorization Process and Cyber AB Accreditation Requirements

After we announced this audit, we received three allegations from the DoD Hotline related to the C3PAO authorization process and the Cyber AB's compliance with a contract requirement to obtain accreditation under ISO/IEC 17011 standards. We substantiated two of the complaints; however, because of actions taken after the complaints were submitted, no additional action was necessary. We did not substantiate the third complaint.

Allegation 1

The DIBCAC did not:

- **provide the candidate C3PAO with assessment guidelines before performing the Level 2 assessment;**
- **review all documentation provided by the candidate C3PAO that supported the implementation of certain NIST SP 800-171 cybersecurity requirements;**
- **provide comments supporting the DIBCAC assessor's determination that certain NIST SP 800-171 cybersecurity requirements were not implemented; and**
- **develop a process to appeal the results of the assessment.**

To assess the allegation, we reviewed email correspondence between the candidate C3PAO and the DIBCAC assessment team related to pre-assessment coordination, the assessment results, and appeals. We also reviewed the assessment report and met with the DIBCAC assessment team to discuss and review the information provided to the candidate C3PAO before and after the assessment and the documentation provided by the C3PAO to the DIBCAC assessment team.

Results

We found that the DIBCAC provided the candidate C3PAO with the assessment guidelines before the assessment; reviewed the documentation that the C3PAO provided; and provided the assessment results to the C3PAO, including comments supporting the DIBCAC assessor's determination that certain cybersecurity requirements were not implemented. However, at the time of the candidate C3PAO's assessment, the DIBCAC had not established an appeals process.

The DIBCAC Provided the Candidate C3PAO with Assessment Guidelines

On August 23, 2022, the DIBCAC assessment team emailed the candidate C3PAO that its Level 2 assessment would begin on December 5, 2022. The assessment team sent the email to the candidate C3PAO 104 days before the scheduled assessment and included a hyperlink to the Level 2 Assessment Guide. The Level 2 Assessment Guide provides guidance on the criteria and methodology the assessment team follows during an assessment.

The DIBCAC Reviewed Documentation Provided by the Candidate C3PAO

Based on our review of the assessment report, the DIBCAC Assessment Lead included notes in the assessment report that indicated that the assessment team reviewed the documentation provided by the candidate C3PAO.

The DIBCAC Assessment Team Included Comments Concerning the Non-Implemented Requirements in the Assessment Report

On December 15, 2022, 6 days after the conclusion of the assessment, the DIBCAC assessment team emailed the candidate C3PAO the preliminary results of the assessment, indicating that they determined the candidate C3PAO had not adequately implemented 23 of the required 110 NIST SP 800-171 requirements.

On January 23, 2023, 45 days after the conclusion of the assessment, the DIBCAC assessment team emailed the candidate C3PAO the final assessment results, including an explanation for each of the NIST SP 800-171 requirements that the DIBCAC concluded were not implemented. For example, the DIBCAC assessors commented that the C3PAO had not implemented the control for "remediating vulnerabilities in accordance with risk assessments," because the candidate C3PAO had never conducted the necessary risk assessments.

The DIBCAC Lacked a Formal Appeals Process but Established an Interim Process Upon the Candidate C3PAOs Request for Appeal

On March 1, 2023, the candidate C3PAO requested that the DIBCAC provide instructions for appealing the results of their DIBCAC assessment. On March 2, 2023, the DIBCAC acknowledged the receipt of the appeals request. Although the DIBCAC did not have a formal appeals process in place at that time, they directed the candidate C3PAO to provide additional information to support the appeal. On March 8 and 20, 2023, the DIBCAC assessment team emailed additional instructions to the candidate C3PAO, requesting that they provide details for each of the requirements that the DIBCAC assessment team indicated was not implemented along with documentation

to support the candidate C3PAO's position that the control should have been considered implemented. On March 22, 2023, the candidate C3PAO provided the assessment team with a list of the requirements and results they disagreed with but did not provide any supporting documentation. Despite the lack of supporting documentation, the DIBCAC reviewed the C3PAO's submission and on April 24, 2023, the assessment team emailed the candidate C3PAO stating that, based on an analysis of the additional information submitted, there was not enough evidence to overturn the initial assessment findings. Although the DIBCAC did not have a formal appeals process in place as of May 11, 2023, the date of the DoD Hotline complaint, we are not making a recommendation to the DIBCAC concerning the complaint because it implemented a formal appeals process on November 21, 2023.[31]

Allegation 2

The Cyber AB did not comply with its contract requirements to obtain accreditation under the ISO/IEC 17011 standards.

To assess the allegation, we reviewed the no-cost contract that the DoD awarded to the Cyber AB in November 2020. In addition, we reviewed the contract that the DoD modified in November 2023. We also met with Cyber AB officials to discuss plans for the Cyber AB to achieve compliance with ISO/IEC 17011 accreditation standards.

Results

As of September 29, 2023, the date of the DoD Hotline complaint, the Cyber AB had not complied with its contract requirement to obtain accreditation under the ISO/IEC 17011 standards by April 30, 2023. However, according to the CMMC PMO Director, the April 30, 2023, suspense date was established in conjunction with the CMMC 1.0 framework. Before publishing the proposed rule for the CMMC 2.0 framework in December 2023, the OCIO modified the Cyber AB contract in November 2023 to require the Cyber AB to obtain accreditation under the ISO/IEC 17011 standards no later than 24 months after the effective date of CMMC 2.0.[32] Therefore, the Cyber AB was compliant with the modified contract requirement.

[31] "DIBCAC Cybersecurity Maturity Model Certification (CMMC) Appeals – Standard Operating Procedures," Initial Release on November 21, 2023.

[32] The expected date for compliance is December 2026, at the earliest.

Allegation 3

During a DIBCAC assessment of a candidate C3PAO, the DIBCAC assessors requested that the candidate C3PAO provide evidence of cybersecurity requirements that are the responsibility of CSPs to implement. The complainant stated that the requested information is included in a security package, maintained by the Federal Government, for all CSPs that government agencies are authorized to use. According to the complainant, the DIBCAC assessors mandated that the candidate C3PAO download the information even though an agreement, which must be signed by package reviewers, states that the security package documentation can only be stored on government furnished equipment. The complainant stated that it appeared that the DIBCAC was unaware of this limitation.

To assess the allegation, we reviewed the candidate C3PAO's responses to the DIBCAC's Assessment Scope Intake Form, which documents information collected from the candidate that supports the candidate's readiness for a Level 2 assessment, including documents related to the use of CSPs. We also reviewed the DIBCAC assessor's notes and met with DIBCAC officials to discuss the methodology used to assess the cybersecurity requirements that were the responsibility of CSPs.

Results

We did not identify evidence indicating that the DIBCAC assessors requested that the candidate C3PAO download the CSP security package documentation to their internal network. Before initiating the Level 2 assessment, the DIBCAC quality assurance lead requested that the candidate C3PAO provide a list of the cybersecurity requirements that their CSPs were responsible for implementing. The quality assurance lead directed the candidate C3PAO to a DoD-developed Frequently Asked Questions document that discusses how contractors should ensure that CSPs meet Federal cybersecurity requirements. The response to that question includes hyperlinks to cybersecurity control templates that companies could use as examples of the type of information needed from the CSP. However, the response from the quality assurance lead did not suggest that the candidate C3PAO download any information related to the CSP cybersecurity requirements and furthermore, our review of the DIBCAC assessor's notes and interviews with DIBCAC officials did not indicate that any member of the DIBCAC assessment team directed the candidate C3PAO to download CSP cybersecurity requirements information to their internal system or network.

Appendix C

Sampling Approach

Sample Selection of C3PAOs

We used a nonstatistical sampling approach to select the C3PAOs to review for this audit. To determine the universe of C3PAOs, we used the Cyber AB Marketplace to identify that the Cyber AB had authorized 48 C3PAOs to perform Level 2 assessments as of September 21, 2023. We copied the list of the 48 C3PAOs in the order they appeared on the Cyber AB Marketplace and pasted the list in Microsoft Excel. Using the "RAND" [random] function in Microsoft Excel, we assigned a random number to each of the 48 C3PAOs. We sorted the list from the highest number to the lowest number based on the random values assigned by Microsoft Excel and selected the 11 C3PAOs with the highest random values.

Sample Selection of DIBCAC Assessments

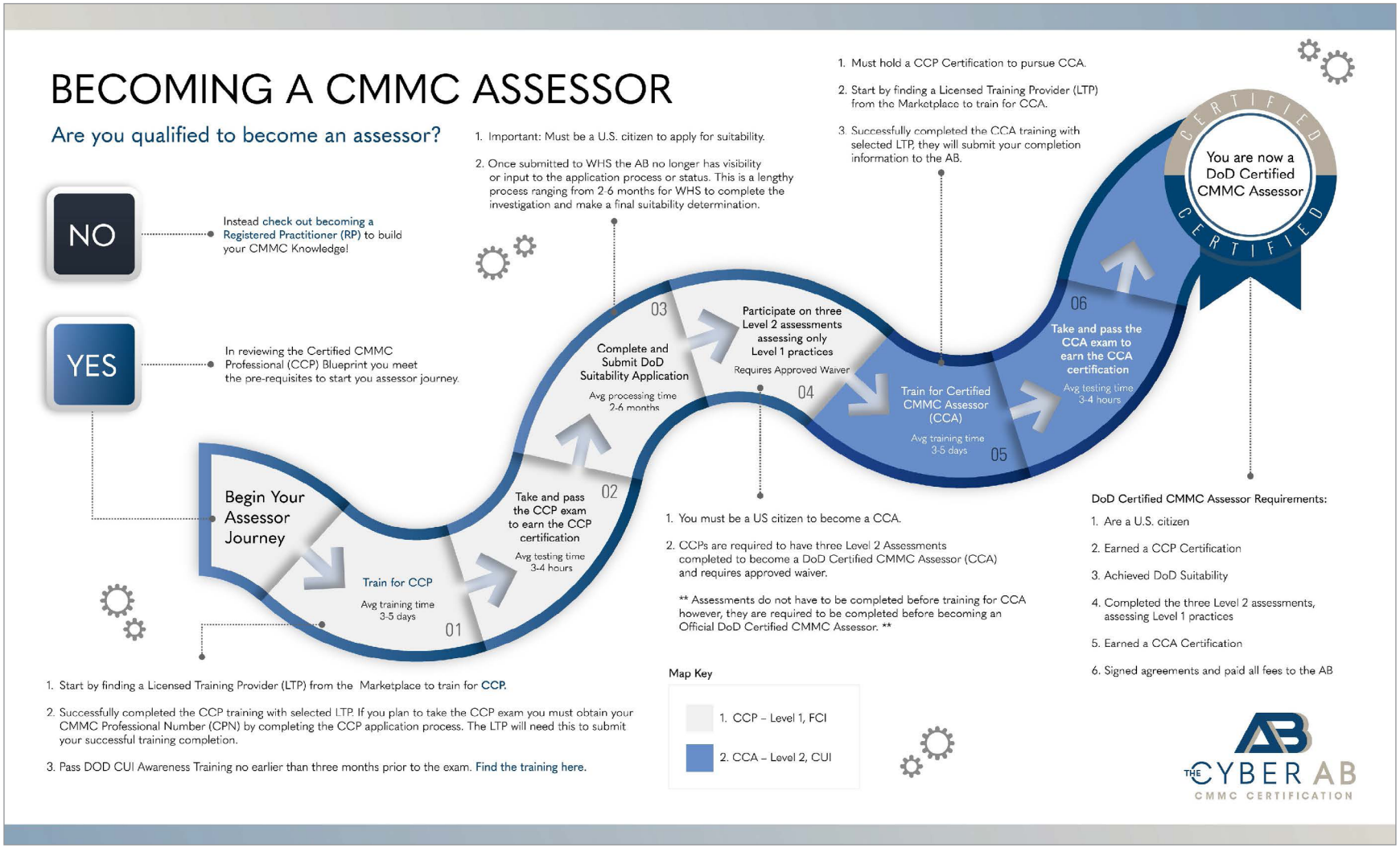
We used a nonstatistical sampling approach to select the DIBCAC Level 2 assessments to observe. To determine the universe of assessments, we requested that the DIBCAC Director provide a schedule of the planned Level 2 assessments of candidate C3PAOs from January through March 2024. We identified that the DIBCAC planned to perform four assessments during that period and based on that universe, we planned to observe all four. However, the DIBCAC recommended to the CMMC PMO that one of the candidate C3PAOs was not ready for an assessment because the C3PAO had misinterpreted the CMMC requirements and objectives. The CMMC PMO agreed, and therefore, we coordinated with DIBCAC officials to observe the remaining three assessments.

Appendix D

CMMC Assessor Training Track

Figure 2 shows the training track to become a CCP and CCA.

Figure 2. CMMC Assessor Training Track



Source: Cyber AB website.

As shown in Figure 2, to achieve CCA certification, individuals must first earn a CCP certification by demonstrating their knowledge of the CMMC framework through a series of Cybersecurity Assessor and Instructor Certification Organization-approved trainings and examinations. Once the DoD confirms that the individual is a U.S. citizen, the individual must attend additional Cybersecurity Assessor and Instructor Certification Organization-approved trainings and pass examinations to obtain certification as a CCA. A QCL is considered certified if they have certifications for both the CCA and CCP.

Management Comments

DoD Chief Information Officer

CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

OCT 22 2024

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment of DoD Inspector General Draft Report "Audit of the DoD's Process for Authorizing Third-Party Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments" (Project No. D2023-D000CR- 0167.000)

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General Draft Report, "Audit of the DoD's Process for Authorizing Third- Party Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments" (Project No. D2023-D000CR-0167.000).

DoD IG RECOMMENDATION 1: The DoD CIO develop and implement a quality assurance process that will ensure that all requirements in the Cybersecurity Maturity Model Certification (CMMC) Third-Party Assessment Organization (C3PAO) authorization process are successfully met before a candidate C3PAO is authorized to perform CMMC Level 2 assessments.

DoD CIO RESPONSE: DoD CIO agrees in part with the DoD IG recommendation.

DoD CIO has included requirements within the contract that CMMC AB must comply with International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standard 17011. This ISO/IEC standard addresses quality assurance compliance and requires completion of a peer evaluation. The CMMC Program is designed to rely on an ISO/IEC standard-compliant Accreditation Body (AB) to oversee the CMMC ecosystem, via contractual oversight by DoD CIO. The DoD's requirements for an AB to oversee the vetting and authorizing of C3PAOs to perform CMMC Level 2 assessments was codified in section 170 of Title 32 of the Code of Federal Regulations (CFR).

DoD IG RECOMMENDATION 2: The CMMC Program Management Office Director direct the contracting officer to modify the contract with the Cyber Accreditation Body to require the CMMC AB to:

a. Verify that the Cyber AB has signed Cybersecurity Maturity Model Certification Third-Party Assessment Organization (C3PAO) Agreements and Codes of Professional Conduct for every authorized C3PAO within 30 days of the date of this report or revoke the C3PAOs authorization to perform CMMC Level 2 assessments until the documents are received.

b. Develop a formalized quality control lead certification requirement.

c. Verify that the quality control leads (QCL) for every authorized Cybersecurity Maturity Model Certification Third-Party Assessment Organization (C3PAO) meet

DoD Chief Information Officer (cont'd)

the certification requirement within 30 days of the date of this report, and, for any of the C3PAO's QCLs who are not certified, revoke the authorization for those C3PAOs to perform CMMC Level 2 assessments until the C3PAOs provide support the QCLs are certified.

d. Verify the employment status of the on-staff CMMC certified assessors and certified quality control leads (QCL) by requesting and reviewing employment records to confirm that CMMC certified assessors and certified QCLs are part of the candidate Cybersecurity Maturity Model Certification Third-Party Assessment Organization's staff and are assigned those specific roles and responsibilities.

e. Verify the employment status of the CMMC certified assessors and certified quality control leads of all previously authorized Cybersecurity Maturity Model Certification Third- Party Assessment Organizations (C3PAO) using the methodology defined in Recommendation 2.d within 30 days of the date of this report and revoke the C3PAO's authorization to perform CMMC Level 2 assessments if the employment status cannot be verified.

DoD CIO RESPONSE: DoD CIO agrees in part with the DoD IG recommendation.

Due to the constraints of formal rulemaking, the CMMC AB was treated as a member of the public and was not provided access to certain decisions made in the requirements development process of the program. The CMMC PMO Director will provide appropriate recommendations to the contracting officer and pursue modification of the contract to align its requirements to the final CMMC Program rule. Normal procurement and contracting procedures will govern the Procurement Action Lead Time, and that timeline will be decided by the contracting officer. Additionally, the CMMC PMO maintains regular and recurring communication with the CMMC AB to discuss contract performance, including progress of C3PAO candidates through the authorization process. Response to the specific recommended contact modifications are as follows:

a. In response to this finding, the CMMC PMO received confirmation from the CMMC AB that all currently authorized C3PAOs have provided the required C3PAO Agreements and Code of Professional Conduct and that the CMMC AB will retain the associated documentation on file. The CMMC PMO Director also requested that the CMMC AB implement a process to report the documentation status of each C3PAO in advance of any future CMMC AB formal authorization. With the CMMC Program is codified in Title 32 of the CFR, the CMMC PMO Director will work with the DoD contracting officer to pursue a contract modification to clarify the reporting desired as part of the CMMC AB's standard C3PAO authorization / reauthorization process. The CMMC PMO Director will initiate this contract modification to ensure efficiency and synchronization with approved final rule content. Completion of the modification will be in accordance with normal procurement lead times. The CMMC Program rule in Title 32 of the CFR will become effective on December 16, 2024. The date of the IG report is immaterial to the authorization process for C3PAOs because until the title 32 CFR CMMC Program rule is codified and effective, C3PAOs are not permitted to perform CMMC assessments.

DoD Chief Information Officer (cont'd)

b. Requirements for a certified Quality Control Lead are not desired or necessary, nor are they part of the currently defined CMMC Program. Instituting such requirements would necessitate significant rulemaking to revise Title 32 of the CFR. These requirements that C3PAOs must implement a Quality Assurance (QA) function are set out in the final rule. The purpose of the QA function is to ensure C3PAO assessment reports are accurately completed in a manner consistent with all assessment guidelines and requirements prior to submission to the DoD. The individual performing the QA function is required to be a Certified CMMC Assessor (CCA) to ensure they have the appropriate technical qualifications and assessment experience. To prevent conflicts of interest, any individual performing the QA function is prohibited from serving as a team member for assessments which they also review for quality assurance.

c. In accordance with Title 32 of the CFR and the DoD's - contract requirements, the CMMC AB subjects C3PAOs to quality assurance reviews. All CMMC AB documentation should use the approved term "Quality Assurance (QA)," and the CMMC AB will be responsible to ensure C3PAO compliance with requirements of the QA function as specified in Title 32 of the CFR. The CMMC PMO Director will pursue modification of the no-cost contract as referenced above to clarify the QA function consistent with the requirement in Title 32 of the CFR.

d./e. The CMMC PMO has established a CMMC assessment ecosystem based on an open market system. As noted above, DoD is limited by the CMMC roles and responsibilities codified in Title 32 of the CFR and forces of an open market CMMC ecosystem. The DoD cannot mandate that individuals assigned to QA functions, or any other staff, be employed as a permanent member of the C3PAO. The DoD has assigned managing and tracking of assessor certification status to the CMMC Assessor and Instructor Certification Organization (CAICO), as defined in Title 32 of the CFR. The CAICO ensures that the certification status of the assessors is managed and conveyed to C3PAOs. As specified in Title 32 of the CFR, the CMMC AB is responsible for ensuring C3PAOs comply with the requirement to use certified assessors and that individuals performing the QA function are CCAs and not members of the team that completed the QA review and report. Assessor certification requirements are set out in Title 32 of the CFR, and those requirements are managed in accordance with ISO/IEC 17024 standards. C3PAO requirements are set out in the final rule of Title 32 of the CFR, and those requirements are managed in accordance with ISO/IEC 17020 standards. Verification of C3PAO staff employment status by the CMMC PMO is, therefore, is governed by contract with the CMMC AB and the C3P AO.

DoD IG RECOMMENDATION 3: The CMMC Program Management Office Director:

a. Develop and implement a formal reauthorization process for the Cybersecurity Maturity Model Certification Third-Party Assessment Organizations (C3PAO) that includes a review and verification for all requirements in the C3PAO authorization process.

DoD Chief Information Officer (cont'd)

b. Develop and implement a process to ensure Cybersecurity Maturity Model Certification Third-Party Assessment Organizations (C3PAO) immediately notify both the CMMC Program Management Office and Cyber Accreditation Body of any changes associated with any of the requirements in the C3PAO authorization process.

c. Revise the CMMC assessment guides to further define the requirement for disabling inactive accounts to include group accounts.

DoD CIO RESPONSE: DoD CIO partially agrees with the DoD IG recommendation 3.

a. The process associated with reauthorization is the same as that for initial authorization. The CMMC PMO Director will pursue addition of a new contract deliverable outlining CMMC AB internal processes for tracking and managing authorization and reauthorization of C3PAOs.

b. The DoD CIO agrees in part with the DoD IG recommendation to require C3PAOs to immediately notify both the CMMC PMO and the CMMC AB of changes associated with any requirement in the C3PAO authorization process. Status as a C3PAO is governed by its relationship with the CMMC AB that enforces such reporting, and Title 32 of the CFR aligns responsibility for managing the C3PAOs to the CMMC AB. As part of the planned modification to the CMMC AB contract, the CMMC PMO Director will pursue revisions to CMMC AB procedures that will result in timely C3PAO notification of any changes associated with C3PAO requirements for authorization, re-authorization, or accreditation to the CMMC AB. The CMMC PMO will also pursue the addition of new contract deliverables for appropriate reporting of such C3PAO notification to the DoD.

c. The DoD CIO partially agrees with the DoD IG's recommendation to revise the assessment guides to further define the requirement for "disabling inactive accounts to include group accounts". There is no need for additional action as the recommendation is in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, which describes disabling "identifiers", which is defined to include a specific "entity, object, or group". The CMMC assessment guides are written to appropriately align to the meaning of the NIST documentation.

A security review to verify "CONTROLLED UNCLASSIFED INFORMATION" (CUI) markings in the report has been completed, and there are no additional recommendations.

The point of contact for this matter is [redacted]. He can be reached at [redacted] or [redacted].

Leslie A. Beavers
Acting

Defense Contract Management Agency

DEFENSE CONTRACT MANAGEMENT AGENCY
3901 ADAMS AVENUE, BUILDING 10500
FORT GREGG-ADAMS, VA 23801-1809

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: DCMA response to the Audit of the DoD's Process for Authorizing Third-Party Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments draft report (Project No. D2023-D000CR-0167.000)

The Defense Contract Management Agency (DCMA) appreciates the opportunity to review and comment on the report. The DCMA partially agrees with Recommendation 4.

The point of contact for this audit is [redacted] DCMA Defense Industrial Base Cybersecurity Assessment Center, Director, [redacted] or email [redacted].

EBRIGHT.SONYA.I [redacted] Digitally signed by [redacted] Date: 2024.10.07 09:01:03 -04'00'

Sonya I. Ebright
Deputy Director

Defense Contract Management Agency (cont'd)

DCMA Management Comments on the Audit of the DoD's Process for Authorizing Third-Party Organizations to Perform Cybersecurity Maturity Model Certification 2.0 Assessments draft report (Project No. D2023-D000CR-0167.000)

DoD OIG RECOMMENDATION 4: We recommend that the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Director require the DIBCAC assessors to retest the requirement for disabling user and group accounts after a defined period of inactivity for every Cybersecurity Maturity Model Certification Third-Party Assessment Organization previously authorized to perform Level 2 assessments.

DCMA RESPONSE: DCMA partially agrees with this recommendation. The DIBCAC will conduct a review for 25% of C3PAO assessments conducted during the last two years and will take appropriate action based upon the results. **Estimated Completion Date: December 13, 2024**

Based upon review of data, DCMA concurs with the DoD OIGs finding that candidate C3PAO One did not define a period of inactivity after which inactive accounts would be disabled. While candidate C3PAO One did not have any inactive accounts noted during the demonstration, lack of a defined policy should have caused this requirement to be scored "Not Met."

DCMA disagrees with the DoD OIG's determination that candidate C3PAO Two should have been scored as "Not Met." The DoD OIG's determination hinges on the candidate C3PAO not having a defined process for group accounts. The candidate C3PAO utilizes a Google Cloud environment which cannot natively have group accounts. A 'group account' is different than a 'group', which is permitted in the Google Cloud environment, however a 'group' is composed of individual accounts. While an account with shared credentials is possible, in a cloud setting, it will violate the Terms of Service established by providers which license by user seats. In addition to the technical limitations of not being able to create a group account, no group accounts were observed by DCMA or DoD OIG in either assessment, therefore, the DIBCAC assessors reviewed all identifiers that were part of the system at the time of each assessment.

The DIBCAC applies a continuous improvement approach within all facets of the organization. Immediate action will include an email on the subject from the DIBCAC Director to the entire organization and a follow-on training during the DIBCACs bi-weekly training session. Our training team will evaluate our existing assessor training course to reiterate that identifiers do include specific entity (user, non-person entity), object (computers, printers, and other devices), or group (distribution groups, and the like) whether it is identified in the System Security Plan (SSP) or observed during the assessment. **Estimated Completion Date: October 18, 2024**

Acronyms and Abbreviations

AB	Accreditation Body
CCA	CMMC Certified Assessor
CCP	CMMC Certified Professional
CMMC	Cybersecurity Maturity Model Certification
CSP	Cloud Service Provider
CUI	Controlled Unclassified Information
C3PAO	CMMC Third-Party Assessment Organization
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
PMO	Program Management Office
QCL	Quality Control Lead
SP	Special Publication

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

www.twitter.com/DoD_IG

LinkedIn
www.linkedin.com/company/dod-inspector-general/

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098