



May 2022

DEFENSE CYBERSECURITY

Protecting Controlled Unclassified Information Systems

Accessible Version

GAO Highlights

Highlights of [GAO-22-105259](#), a report to Congressional Committees

Why GAO Did This Study

DOD computer systems contain vast amounts of sensitive data, including CUI that can be vulnerable to cyber incidents. In 2015, a phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in an 11-day shutdown while cyber experts rebuilt the network. This affected the work of roughly 4,000 military and civilian personnel.

In response to Section 1742 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, in June 2021 DOD submitted a report to the Congress on cybersecurity of CUI. The report discussed the extent to which DOD had implemented selected cybersecurity requirements across the department. The act included a provision for GAO to review DOD's report, and GAO has continued to monitor the department's subsequent progress.

This report describes 1) the status of DOD components' implementation of selected CUI cybersecurity requirements; and 2) actions taken by DOD CIO to address the security of CUI systems.

GAO's review focused on the department's approximately 2,900 CUI systems. GAO examined relevant CUI cybersecurity requirements and data from DOD information technology tools. Also, GAO analyzed documentation such as relevant DOD cybersecurity policies and guidance on monitoring the implementation of cybersecurity requirements, and interviewed DOD officials.

DOD provided technical comments on a draft of this report, which GAO incorporated as appropriate.

View [GAO-22-105259](#). For more information, contact Joseph Kirschbaum at kirschbaumj@gao.gov or (202) 512-9971 or Jennifer R. Franks at franksj@gao.gov or (404) 679-1831.

May 2022





DEFENSE CYBERSECURITY

Protecting Controlled Unclassified Information Systems

What GAO Found

The Department of Defense (DOD) has reported implementing more than 70 percent of four selected cybersecurity requirements for controlled unclassified information (CUI) systems, based on GAO's analysis of DOD reports (including a June 2021 report to Congress) and data from DOD's risk management tools. These selected requirements include (1) categorizing the impact of loss of confidentiality, integrity, and availability of individual systems as low, moderate, or high; (2) implementing specific controls based in part on the level of system impact; and (3) authorizing these systems to operate. As of January 2022, the extent of implementation varied for each of the four requirement areas. For example, implementation ranged from 70 to 79 percent for the cybersecurity maturity model certification program DOD established in 2020, whereas it was over 90 percent for authorization of systems to operate (see table).

Implementation of Selected Requirements for DOD Controlled Unclassified Information Systems, as of January 2022

	Fully compliant with CUI requirement	Department of Defense
Categorize DOD CUI systems accurately	No	 80% to 89%
Implement Cybersecurity Maturity Model Certification's 110 security requirements	No	 70% to 79%
Implement 266 security controls for moderate confidentiality impact systems	No ^a	 80% to 89%
Authorize system to operate on DOD network	No	 90% or more

Source: GAO analysis of Department of Defense (DOD) data. | [GAO-22-105259](#)

Accessible Information for Implementation of Selected Requirements for DOD Controlled Unclassified Information Systems, as of January 2022

Category	Fully compliant with CUI Requirement	Department of Defense
Categorize DOD CUI systems accurately	No	80% to 89%
Implement Cybersecurity Maturity Model Certification's 110 security requirements	No	70% to 79%
Implement 266 security controls for moderate confidentiality impact systems	No	80% to 89%
Authorize system to operate on DOD network	No	90% or more

^aDOD is not required to implement all 266 security controls. In some cases, a specific security control may not be applicable to a particular system due to its function. Also, there are some systems for which the authorizing officials may need to implement security controls that are in addition to the 266 identified as moderate-impact for confidentiality because of the type of information that is stored or transmitted in that system.

As the official responsible for department-wide cybersecurity of CUI systems, the DOD Office of the Chief Information Officer (CIO) has taken recent action to address this area. Specifically, in October 2021 the CIO issued a memorandum on implementing controls for CUI systems. The memo identified or reiterated requirements that CUI systems must meet. These included requiring additional supply chain security controls and reiterating that all CUI systems have valid authorizations to operate. In addition, the CIO reminded system owners of the March 2022 deadline for all DOD CUI systems to implement necessary controls and other requirements. The Office of the CIO has been monitoring DOD components' progress in meeting this deadline.

Contents

GAO Highlights	ii
Why GAO Did This Study	ii
What GAO Found	ii
Letter	1
Background	4
DOD Has Partially Implemented Selected CUI Cybersecurity Requirements	7
DOD Office of the CIO Has Taken Action to Address Security of DOD's CUI Systems	11
Agency Comments	14
Appendix I: Objectives, Scope, and Methodology	17
Appendix II: Comments from the Department of Defense	21
Accessible Text for Appendix II: Comments from the Department of Defense	23
Appendix III: GAO Contacts and Staff Acknowledgments	24

Figures

Figure 1: Comparison of the DOD Risk Management Framework and the Cybersecurity Maturity Model Certification (CMMC) 2.0 Framework	7
Figure 2: Implementation of Selected Cybersecurity Requirements for Department of Defense's (DOD) Controlled Unclassified Information (CUI) Systems, as of January 2022	8
Accessible Information for Figure 2: Implementation of Selected Cybersecurity Requirements for Department of Defense's (DOD) Controlled Unclassified Information (CUI) Systems, as of January 2022	8

Abbreviations

C.F.R.	Code of Federal Regulations
CIO	Office of the Chief Information Officer
CMMC	Cybersecurity Maturity Model Certification
CNSSI	Committee on National Security Systems Instruction
CUI	Controlled unclassified information

DFARS	Defense federal acquisition regulation supplement
DOD	Department of Defense
eMASS	Enterprise Mission Assurance Support Service
IT	Information Technology
MCCAST	Marine Corps Compliance and Authorization Support Tool

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



May 19, 2022

Congressional Committees

Recent cyber incidents at federal agencies demonstrate the damage that malicious cyber actors can cause. These cyber incidents reinforce the importance of effectively protecting federal systems, including those used by the Department of Defense (DOD). Many of these systems contain vast amounts of sensitive data, thus making it imperative to protect them. For example:

- Between May and July 2019, the Defense Information Systems Agency network was breached, potentially compromising personally identifiable information of their employees, including Social Security numbers.
- In July 2015, a phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in an 11-day shutdown while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel.¹

Controlled unclassified information (CUI) is created or possessed by the government or by an entity for or on behalf of the government. Applicable law, regulation, or government-wide policy requires or permits an agency to handle CUI using safeguarding or dissemination controls.² CUI may include data related to critical technologies, such as elements of artificial intelligence and biotechnology, and information relating to the design, development, and operations of weapons and defense-critical infrastructure. Due to the sensitive nature of CUI, additional cybersecurity protections are required. For example, in March 2020, DOD established the Cybersecurity Maturity Model Certification (CMMC) framework, which

¹Center for Strategic and International Studies, *Significant Cyber Incidents since 2006* (2019). Phishing is a digital form of social engineering in which adversaries send hyperlinks in authentic-looking, but fake, emails to direct users to fake websites that download malware onto users' networks and collect sensitive information from users. Malware is malicious software intended to perform an unauthorized process that will have an adverse effect on the confidentiality, integrity, or availability of an information system. Examples of sensitive information are usernames and passwords.

²32 C.F.R. § 20002.4 (h).

established requirements for defense contractors that store or transmit DOD CUI data.

Safeguarding federal computer systems has been a longstanding concern. Underscoring the importance of this issue, we have included cybersecurity on our high-risk list since 1997.³ In March 2021, we recommended that officials move with a greater sense of urgency to address four major cybersecurity challenges and 10 associated critical actions commensurate with the rapidly evolving and grave threats to the country.⁴

In June 2021—in response to Section 1742 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (hereafter referred to as FY 2021 NDAA)—DOD submitted a report to the Congress on the cybersecurity of CUI. The report described the extent to which DOD had implemented selected cybersecurity requirements across the department. Section 1742 also included a provision for us to review DOD’s report and provide a briefing to the congressional defense committees no later than 180 days after the submission of DOD’s report.⁵ We reviewed DOD’s report, briefed the House Armed Services Committee in September 2021 on the preliminary observations of our review, and have continued to monitor the department’s subsequent progress.

This report describes 1) the status of DOD components’ implementation of selected CUI cybersecurity requirements; and 2) actions taken by the DOD Office of the Chief Information Officer (CIO) to address the security of DOD’s CUI systems.

³See GAO, *High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas*, [GAO-21-119SP](#) (Washington, D.C.: Mar. 24, 2021); and *High-Risk Series: An Overview*, [GAO-HR-97-1](#) (Washington, D.C.: Feb. 1, 1997). GAO maintains a high-risk program to focus attention on government operations that it identifies as high risk due to their greater vulnerabilities to fraud, waste, abuse, and mismanagement or the need for transformation to address economy, efficiency, or effectiveness challenges.

⁴See GAO, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, [GAO-21-288](#) (Washington, D.C.: Mar. 24, 2021).

⁵Pub. L. No. 116-283, § 1742 (2021).

For the purpose of this report, the scope of our analysis is focused on approximately 2,900 CUI systems across the department. Five DOD components own about 85 percent of the department's CUI systems. The components are: Army, Air Force, Defense Health Agency, Marine Corps, and Navy. The remaining 32 components are hereafter grouped together and referred to as "Other".⁶ Some examples of these remaining components include: the Office of the Secretary of Defense, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the DOD agencies (e.g., the Defense Logistics Agency), and the DOD field activities (e.g., Washington Headquarters Services).

To address our objectives, we reviewed relevant CUI cybersecurity requirements and data from DOD information technology tools, and interviewed and corresponded with knowledgeable officials. We also assessed the reliability of the cybersecurity data by reviewing the methods that the DOD CIO and Marine Corps use to ensure the data reported are accurate and by interviewing cognizant officials. We found that the security control data we examined were sufficiently reliable for describing how DOD components implemented CUI security controls.⁷ We also obtained and analyzed documentation, conducted interviews, and reviewed relevant DOD and federal cybersecurity policies and guidance related to the CMMC framework and DOD's efforts to monitor the implementation of cybersecurity requirements. For a detailed description of our objectives, scope, and methodology, see appendix 1.

We conducted this performance audit from May 2021 to May 2022 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.

⁶Although DOD has 45 components, our analysis includes data based on 37 components. We excluded eight components because their compliance data are maintained in classified systems. The eight are: the Joint Improvised-Threat Defeat Organization, Missile Defense Agency, and White House Communications Agency, Defense Intelligence Agency, Defense Legal Services Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency.

⁷The compliance range for the Marine Corps is not comparable to the other components because their data excluded a small percentage of the required security controls due to ongoing changes to Marine Corps systems that are designated as CUI systems.

Background

Requirements to Protect DOD CUI

Federal regulations and policies establish the requirements for both federal agencies—including DOD— and non-federal organizations to protect CUI that is processed, transmitted, or stored in their respective information systems. For example, part 2002 of Title 32, Code of Federal Regulations (C.F.R.) describes the executive branch’s CUI program and establishes policy for designating and handling CUI information.

Specifically,

- Section 2002.14 (g) states that information systems that process, store, or transmit CUI be categorized no less than the moderate confidentiality impact level in accordance with FIPS PUB 199.⁸ According to FIPS PUB 199, the potential impact is moderate if the loss of confidentiality, integrity or availability⁹ could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.¹⁰ Section 2002.14 (h)(2) also states that non-federal information systems of organizations that process, transmit, or store CUI are generally governed by the requirements of National Institute of Standards and Technology Special Publication 800-171.¹¹ This latter requirement, applicable

⁸32 C.F.R. Part 2002 (2022). Security categorization for information systems identifies the potential impact (low, moderate, or high) that can result from loss of confidentiality, integrity, or availability of a system and the highest value for each type of information resident on the system. Federal agencies are required to identify three impact levels affecting confidentiality: low, moderate, and high. The levels refer to the expected adverse effects on organizational operations, organizational assets, or individuals.

⁹FIPS PUB 199 defines confidentiality as preserving authorized restrictions on information access and disclosure. It defines integrity as guarding against improper modification or destruction. It defines availability as ensuring reliable and timely access to and use of information.

¹⁰Federal Information Processing Standards Publication 199: *Standards for Security Categorization of Federal Information and Information Systems* (February 2004). (FIPS PUB 199).

¹¹32 C.F.R. 2002.14 (h)(2).

specifically to defense contractors, is included in DOD's defense federal acquisition regulation supplement (DFARS).¹²

- DOD Instruction 8510.01 requires DOD to select controls in accordance with guidance from the Committee on National Security Systems Instruction No. 1253.¹³ The instruction also requires DOD systems to undergo a prescribed risk management framework process and be reauthorized to operate on DOD's information network every 3 years. Any system that does not complete this reauthorization process is not considered "authorized to operate."
- DOD established the Cybersecurity Maturity Model Certification (CMMC) program in 2020, as a framework to enhance the protection of unclassified information, such as federal contract information and CUI that resides on information systems within the Defense Industrial Base sector.¹⁴ In November 2021, DOD released a revised CMMC 2.0 framework. According to DOD, the changes reflected in CMMC 2.0 will be implemented through the rulemaking process (Part 32 of the C.F.R. and DFARS) and defense contractors will be required to comply once the forthcoming rules go into effect. For organizations whose systems process, transmit, or store DOD CUI, their systems are expected, among other things, to be compliant with NIST Special Publication 800-171.¹⁵

¹²Defense Federal Acquisition Regulation Supplement section 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting* (as of December 2019).

¹³DOD Instruction 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)* (Mar. 12, 2014, Incorporating Change 3, Dec. 29, 2020); Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems* (Mar. 27, 2014). This guidance builds on and is a companion document to National Institute of Standards and Technology Special Publication, 800-53, *Security and Privacy Controls for Information Systems and Organizations*. For example, CNSSI No. 1253 instructs the usage of the National Institute of Standards and Technology guidance in identifying the information types and selecting a baseline set of security controls.

¹⁴DOD, *Cybersecurity Maturity Model Certification ver 1.02* (March 18, 2020); Defense Federal Acquisition Regulation Supplement: *Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)*, 85 Fed. Reg. 61505 (Sep. 29, 2020). DOD generally refers to the CMMC program that was established in 2020 as CMMC 1.0.

¹⁵National Institute of Standards and Technology Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Revision 2 (Gaithersburg, Md.: February 2020).









DOD's Report to Address Section 1742

Under section 1742 of the FY 2021 NDAA, DOD was required to submit a report to identify whether each component's information systems that process, store, or transmit CUI meet the same security control requirements as the CMMC framework.¹⁶ For each DOD component that did not meet the CMMC security control requirements, section 1742 required a determination and details on how the component will implement those security measures by March 2022 and how the component will mitigate potential risks until those measures are implemented.

In response to this statutory requirement, DOD issued a report on June 30, 2021, that used the DOD Risk Management Framework—and not the CMMC framework—to identify the extent to which DOD components were meeting security requirements to protect CUI. The DOD Risk Management Framework as described in DOD Instruction 8510.01 and the CMMC framework are different models—the former based on risk and the latter on compliance (see figure 1).

¹⁶Section 1742 required DOD to assess itself against the CMMC framework. The CMMC 1.0 framework established by DOD in 2020 initially included five maturity levels. In the CMMC 1.0 framework, DOD would have required defense contractors that process, store, or transmit CUI to meet "level 3". Level 3 would have required a defense contractor to meet 130 security requirements and three capabilities (e.g., issue a security plan for each information system). In December 2021, DOD issued the CMMC 2.0 framework that reduces the five maturity levels to three maturity levels and incorporates requirements from NIST SP 800-171 and NIST SP 800-172. If implemented, under CMMC 2.0, defense contractors that process, store, or transmit CUI would be expected to meet "level 2", which is composed of 110 security requirements. Since DOD introduced the CMMC version 2.0 framework during our review, we assessed DOD against this version of the framework.

Figure 1: Comparison of the DOD Risk Management Framework and the Cybersecurity Maturity Model Certification (CMMC) 2.0 Framework

DOD Risk Management Framework Applicable to DOD components	CMMC 2.0 Framework Applicable to defense contractors
 Risk-based framework	 Compliance-based framework
 266 <i>optional</i> security controls selected based on risk	 110 <i>mandatory</i> security requirements
 Plans of Action and Milestones <i>allowed</i> for systems that do not comply with security controls	 <i>Limited allowance</i> of Plans of Action and Milestones for systems that do not comply with security controls ^a
 Does not have waiver restrictions	 Very limited use of waivers with restrictions to mitigate Controlled Unclassified Information (CUI) risk

Source: GAO analysis of Department of Defense (DOD) information. | GAO-22-105259

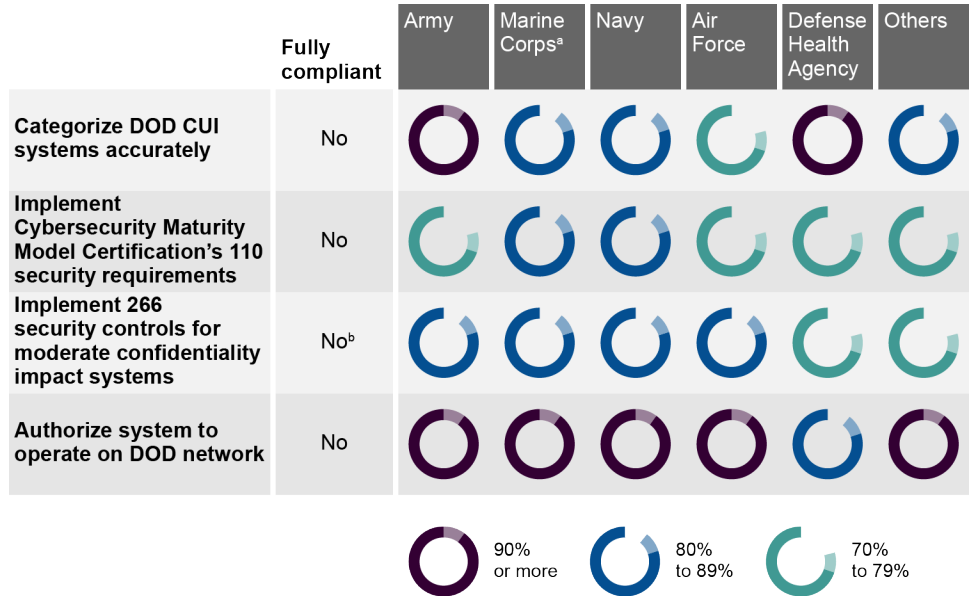
^aAccording to DOD's CMMC documents, the department intends to limit the use of plans of action and milestones by limiting the duration (potentially 180 days), not allowing plans of action and milestones for highest-weighted requirements, and establishing a minimum-score requirement.

DOD Has Partially Implemented Selected CUI Cybersecurity Requirements

Our analysis of DOD-reported data determined that DOD components have taken actions to implement selected cybersecurity requirements for CUI systems, but none were fully compliant. DOD is working toward achieving 100 percent compliance in three of the four categories applicable to the department: categorize systems accurately, implement 266 security controls, and authorize systems to operate on DOD's network (as shown in figure 2).¹⁷

¹⁷DOD is not required to comply with CMMC (i.e., NIST Special Publication 800-171). However, we included it in our analysis based on the Section 1742 requirement for DOD to assess its components against this cybersecurity framework.

Figure 2: Implementation of Selected Cybersecurity Requirements for Department of Defense's (DOD) Controlled Unclassified Information (CUI) Systems, as of January 2022



Source: GAO analysis of Department of Defense (DOD) data. | GAO-22-105259

Accessible Information for Figure 2: Implementation of Selected Cybersecurity Requirements for Department of Defense's (DOD) Controlled Unclassified Information (CUI) Systems, as of January 2022

Category	Fully compliant	Army	Marine Corps	Navy	Air Force	Defense Health Agency	Others
Categorize DOD CUI systems accurately	No	90% or more	80% to 89%	80% to 89%	70% to 79%	90% or more	80% to 89%
Implement Cybersecurity Maturity Model Certification's 110 security requirements	No	70% to 79%	80% to 89%	80% to 89%	70% to 79%	70% to 79%	70% to 79%
Implement 266 security controls for moderate confidentiality impact systems	No	80% to 89%	80% to 89%	80% to 89%	80% to 89%	70% to 79%	70% to 79%
Authorize system to operate on DOD network	No	90% or more	90% or more	90% or more	90% or more	80% to 89%	90% or more

Note: DOD's requirement is 100 percent compliance in the latter three categories. This analysis reflects GAO's assessment of the extent to which DOD CUI systems met selected cybersecurity requirements for CUI systems, as of January 2022. For the requirements related to implementation of security controls, our assessment did not include security controls that DOD identified as not applicable.

^aThe Marine Corps' range of compliance excluded 8 percent of the Cybersecurity Maturity Model Certification (CMMC) security requirements and 11 percent of the moderate-impact confidentiality security controls due to ongoing changes to Marine Corps systems that are designated as CUI systems.

^bDOD is not required to implement all 266 security controls. In some cases, a specific security control may not be applicable to a particular system because of the type of information that is stored or transmitted in that system (e.g., a radio system).

Additional details on the categories are described below.

Categorize DOD CUI systems accurately. Based on the risk management framework that DOD uses to manage risks to information technology systems, the first step a DOD component should take is to categorize the impact level of the system. System categorization identifies the potential impact (low, moderate, or high) that can result from loss of confidentiality, integrity, or availability of a system and its information. At a minimum, the standard for federal systems that process, store, or transmit CUI is a moderate-impact confidentiality level, according to 32 C.F.R. § 2002.14 (g).¹⁸ As of January 2022, DOD CIO officials reported that DOD components had incorrectly categorized 13 percent of its CUI systems below the moderate-impact confidentiality level.¹⁹ As shown in figure 2 above, we found that the Defense Health Agency accurately categorized more than 90 percent of its CUI systems whereas the Air Force inaccurately categorized the impact level for more than 20 percent of their respective systems.

Implement CMMC's 110 requirements. DOD's CMMC version 2.0 program, if implemented, will require defense contractors whose systems process, transmit, or store DOD CUI to be compliant with NIST Special Publication 800-171 in order to achieve level 2, advanced cybersecurity.

DOD's cybersecurity data reflected that DOD components' CUI systems were compliant with 78 percent of the 110 security controls that CUI

¹⁸32 C.F.R. § 2002.14 (g) (2022).

¹⁹DOD Instruction 8510.01 requires that programs for all systems categorize and select controls—the first two steps in the DOD risk management framework—in accordance with CNSSI No. 1253. In the categorization process, the information owner identifies the potential impact (low, moderate, or high) resulting from loss of confidentiality, integrity, and availability if a security breach occurs.

systems of defense contractors must meet under DOD's proposed CMMC version 2.0 program. However, DOD's components' systems would not be approved to process, transmit, or store DOD CUI if CMMC version 2.0 applied to the components. This is because CMMC would require defense contractors to comply with all 110 security controls to achieve level 2, advanced cybersecurity. As of January 2022, the DOD components had not met 22 percent of the 110 security controls. Specifically, we found that the Marine Corps and the Navy CUI systems were compliant with more than 80 percent but less than 90 percent of the CMMC-required security controls for their systems while the other four DOD components were compliant with more than 70 percent but less than 80 percent.

Implement 266 security controls for moderate confidentiality impact systems. To achieve the required moderate-impact confidentiality level, DOD officials who authorize information systems are supposed to select applicable security controls from a list of 266 security controls.²⁰ As of January 2022, DOD CIO officials had found DOD components were compliant with 82 percent of moderate-impact confidentiality controls. As shown in figure 2 above, we found that the Air Force, Army, Marine Corps, and Navy were compliant with more than 80 percent but less than 90 percent of moderate-impact baseline confidentiality controls, while the Defense Health Agency and Other components were non-compliant with more than 20 percent of the moderate-impact baseline confidentiality controls.

Authorize system to operate on DOD network. DOD's risk management framework and NIST's guidance require a system, before it is connected to the DOD network, to undergo an assessment of its security and residual risk.²¹ If the results of this assessment are acceptable to the authorizing official, the system is granted an

²⁰CNSSI No. 1253 identifies 266 security controls; however, DOD authorizing officials do not have to implement all 266 security controls. In some cases, a specific security control may not be applicable to a particular system. Also, there are some systems that may need to implement security controls that are in addition to the 266 identified as moderate-impact for confidentiality because of the type of information that is stored, transmitted, or at rest in that system.

²¹DOD Instruction 8510.01.

authorization to operate on DOD's network.²² As a part of the risk management process, DOD systems are to be reauthorized to operate on DOD's networks every 3 years.

In its section 1742 report to Congress, DOD CIO officials reported that most of its CUI systems still had a valid authorization to operate. As shown in figure 2 above, we found that more than 90 percent of the Army's, Air Force's, Navy's, Marine Corps', and "Other DOD components" CUI systems had a valid authorization to operate. However, 7 percent of DOD's systems did not have a valid authorization to operate. For example, the Defense Health Agency had more than 10 percent of its CUI systems operating without a valid authorization.

DOD Office of the CIO Has Taken Action to Address Security of DOD's CUI Systems

DOD Office of the CIO Issued Guidance on CUI Requirements

In October 2021, the Deputy CIO for Cybersecurity issued a memorandum titled *Requirement for Applying Baseline Controls for Controlled Unclassified Information Systems*. This memorandum defines requirements that DOD's CUI systems must meet and establishes a deadline for compliance of March 2022. As of February 2022, approximately 80 percent of DOD CUI systems had met the requirements. The memorandum addresses the following areas:

Defines minimum impact categorization requirements for CUI systems. According to DOD Instruction 8510.01, the first step a DOD component should take when authorizing or reauthorizing a system to connect to DOD's network is to categorize the impact-level of a system. The October 2021 memorandum requires CUI information systems to be categorized at no less than a moderate impact level for both confidentiality and integrity. In contrast, 32 C.F.R. § 2002.14 (g) requires CUI information systems to be categorized at no less than the moderate

²²An authorizing official is a senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. The official determines whether the risks to organizational operations, organizational assets, individuals, and other organizations are acceptable. DOD officials stated that the officials responsible for granting authorization are generally component leadership or senior staff.

impact level for confidentiality. The memorandum added an additional requirement beyond standard DOD protections that CUI systems must meet, which is that the CUI system must meet moderate-impact for integrity level. Despite this addition, DOD CIO officials stated that they did not expect the memorandum to change how components approach risk management and how they secure their systems. Components may still choose not to take certain security actions if the individual authorizing the system deems the risk as acceptable.

The memorandum also states that requiring CUI systems to meet moderate confidentiality and moderate integrity will ensure that DOD CUI systems are compliant with security controls at levels that will mirror the practices and capabilities of the CMMC framework for level 3.²³ As of February 2022, more than two-thirds of DOD components' CUI systems had the required impact ratings for confidentiality and integrity, according to DOD CIO documentation.

Requires additional supply chain security controls. The memorandum requires six controls from NIST Special Publication 800-53 to protect an agency's information systems from supply chain threats during its lifecycle, in addition to the moderate-impact confidentiality controls.²⁴ These controls include items such as employing acquisition strategies for the purchase of information technology systems and reviewing suppliers before entering into contracts.

NIST Special Publication 800-53 identifies four of the six controls as part of a baseline of security controls that moderate-impact level systems should be implementing.²⁵ The guidance document that DOD uses for selecting security controls²⁶ has not yet been updated to reflect NIST's

²³The CMMC 1.0 framework established by DOD in 2020 initially included five maturity levels. In the CMMC 1.0 framework, DOD would have required organizations that process, store, or transmit CUI to meet "level 3". Level 3 would have required an organization to meet 130 security requirements and three capabilities (e.g., issue a security plan for each information system).

²⁴NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5 (September 2020).

²⁵NIST Special Publication 800-53B, *Control Baselines for Information Systems and Organizations*, (September 2020).

²⁶CNSS, *Security Categorization and Control Selection for National Security Systems*, CNSSI 1253 (Ft. Meade, Md.: March 2014).

guidance document. However, CIO officials told us they intend to update the guidance to reflect the new requirement.

Reiterates requirement of valid authorizations for CUI systems. The October 2021 memorandum directs the components to ensure that information systems that process CUI have a valid authorization to operate.

In creating DOD's Section 1742 report, DOD CIO officials discovered more than 150 CUI systems that did not have valid authorizations. The memorandum reiterates that information systems that process CUI should have valid authorizations. A valid authorization ensures that the agency has reviewed the risks to the system and determined whether it should be allowed to operate on DOD's networks. DOD officials stated that the officials responsible for granting authorization were generally component leadership or senior staff. As of February 2022, most DOD components' systems had a valid authorization, according to DOD CIO documentation.

Includes a timeline for compliance. The October 2021 memorandum requires all CUI systems to comply with these requirements by March 1, 2022, consistent with section 1742 of the FY 2021 NDAA. If a system will be unable to meet the March timeline, the component must update the CUI system level's plan of action and milestone template by January 17, 2022, with a scheduled completion date of no later than January 1, 2027. As of February 2022, DOD reported that approximately 20 percent of CUI systems had not met the requirements and officials had not developed associated corrective-action plans. According to DOD officials, noncompliant systems will continue to operate while officials implement their corrective-action plans. DOD officials also stated that the 5-year completion period will account for possible budget issues during remediation.

DOD Has Monitored Progress on CUI Requirements

According to officials in the DOD CIO office, the department has regularly monitored DOD components' progress toward implementing CUI cybersecurity requirements to reach the March 1, 2022, deadline. For example, DOD CIO told us they host biweekly meetings with the components' Chief Information Security Officers and weekly meetings with components' authorizing officials to encourage compliance. During these meetings, the DOD CIO typically provided information on the components' progress toward the March compliance deadline. DOD CIO

officials stated that this encouraged the Chief Information Security Officers to make it a priority to meet the requirement.

In addition, according to agency officials, the DOD CIO office has used a number of oversight mechanisms to track DOD's compliance with other cybersecurity requirements or with the implementation of cybersecurity initiatives. For example, DOD's section 1742 report states that the department has conducted standardized, recurring inspections of its components to monitor and track cybersecurity implementation and system authorization. According to DOD, these inspections provided DOD components with a greater understanding of the operational risk that their missions face because of their cybersecurity posture.

Agency Comments

We provided a draft of this report to DOD for review and comment. DOD provided technical comments, which we incorporated as appropriate. The department's written responses are reproduced in appendix II.

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

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



Joseph W. Kirschbaum
Director, Defense Capabilities and Management



Letter

Jennifer R. Franks
Director, Information Technology and Cybersecurity
Center for Enhanced Cybersecurity

List of Committees

The Honorable Jack Reed
Chairman
The Honorable James M. Inhofe
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Jon Tester
Chairman
The Honorable Richard C. Shelby
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

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

The Honorable Betty McCollum
Chair
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

Our objectives were to describe 1) the status of Department of Defense (DOD) components' implementation of selected Controlled Unclassified Information (CUI) cybersecurity requirements; and 2) actions taken by the DOD Office of the Chief Information Officer (CIO) to address the cybersecurity of CUI systems.

DOD components include the Office of the Secretary of Defense, the military departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the defense agencies, the DOD field activities, and all other organizational entities within DOD. For the purpose of this report, the scope of our analysis is focused on approximately 2,900 CUI systems across the department. Five DOD components own about 85 percent of the department's CUI systems—Army, Air Force, Defense Health Agency, Marine Corps, and Navy. The 32 remaining components are hereafter referred to as “Other”.¹

For objective one, we reviewed federal regulations and policies that establish the requirements for federal agencies—including the DOD—to protect CUI that is processed, transmitted, or stored in federal information systems. We also reviewed CUI requirements from DOD guidance. Based on this review, we selected four CUI cybersecurity requirements:

1. accurate categorization of CUI systems
2. implementation of Cybersecurity Maturity Model Certification 2.0 (CMMC) 110 security requirements,
3. implementation of moderate-impact confidentiality requirements, and

¹“Other” refers to the components beyond the five that are specified. Although DOD has 45 components, our analysis includes data based on 37 components. We excluded eight components because their compliance data are maintained in classified systems. The eight are: the Joint Improvised-Threat Defeat Organization, Missile Defense Agency, and White House Communications Agency, Defense Intelligence Agency, Defense Legal Services Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, and the National Security Agency.

4. authorization of CUI systems to operate on DOD's network.²

We evaluated compliance data provided for five components and the "Other" category against selected CUI cybersecurity requirements. To better understand DOD's Section 1742 report, we interviewed officials from DOD's Office of the Chief Information Officer.

To describe the extent to which DOD's components (i.e., the five components and 32 remaining "others") implemented the CMMC 2.0 framework requirements,³ we reviewed CMMC guidance to identify the CMMC level 2 controls that correspond to National Institute of Standards and Technology (NIST) Special Publication 800-171.⁴ NIST 800-171 recommends 110 security requirements for protecting the confidentiality of CUI. We completed a comparison crosswalk of these requirements to the applicable security controls in NIST Special Publication 800-53 and identified 127 baseline security controls.⁵ We did not verify components' compliance with security controls due to the significant investment in time and resources required to do so, given the large volume of data and number of CUI systems across DOD.

For the Army, Air Force, Defense Health Agency, Navy, and Other DOD components, we obtained and analyzed data from DOD's information technology (IT) tool for managing the risk management framework—the Enterprise Mission Assurance Support Service, hereafter referred to as eMASS. The Marine Corps uses a separate IT tool for managing the risk management framework—the Marine Corps Compliance and Authorization Support Tool, hereafter referred to as MCCAAT. We used data from eMASS and MCCAAT to assess the DOD components' efforts

²DOD, *Section 1742, NDAA FY21 DOD Cyber Hygiene and Cybersecurity Maturity Model Certification Framework*, (July 2021).

³We assessed DOD's components against the requirements of the CMMC 2.0 framework. DOD's report used the DOD Risk Management Framework—and not the CMMC framework—to identify the extent to which DOD components were meeting security requirements to protect CUI, as required by section 1742 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. DOD has introduced CMMC 2.0 as the new framework intended for defense contractors.

⁴DOD, *Cybersecurity Maturity Model (CMMC) Model Overview*, Version 2.0 (December 2021); National Institute of Standards and Technology Special Publication 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, Revision 2 (February 2020).

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

to implement the 127 NIST 800-53 security controls that correspond to the NIST Special Publication 800-171 Revision 2 security requirements. We did not include in our assessment the security controls that the DOD components identified as not applicable.

The CMMC compliance range for the Army, Air Force, Defense Health Agency, Navy, and Other DOD components reflect our assessment of data, as of January 2022. The CMMC compliance range for the Marine Corps is not comparable to the other components because their data excluded 8 percent of the required security controls. A Marine Corps official attributed the exclusions to ongoing changes to Marine Corps systems that are designated as CUI systems. The Marine Corps' CMMC compliance range reflects our assessment of data, as of January 2022. DOD is not required to comply with CMMC (i.e., NIST Special Publication 800-171). However, we included it in our analysis based on the section 1742 provision that required DOD to assess its components against those cybersecurity requirements.

To describe the extent to which DOD's components implemented moderate-impact confidentiality requirements, we reviewed the Committee on National Security Systems Instruction (CNSSI) No. 1253 to identify the baseline security controls for a system categorized with moderate impact for confidentiality.⁶ According to CNSSI 1253, there are 266 security controls applicable to this categorization. We did not verify components' compliance of security controls due to the significant investment in time and resources required to do so, given the large volume of data, and the number of CUI systems across DOD.

Also, we obtained and analyzed data from eMASS—to assess the DOD components' efforts—specifically those of the Army, Air Force, Defense Health Agency, Navy, and Other—to implement security controls for CUI systems. We obtained and analyzed Marine Corps data from MCCASt. We determined a range of compliance for each component, as of January 2022. The compliance range for the Marine Corps is not comparable to the other components because their data excluded 11 percent of the moderate-impact confidentiality security controls. A Marine Corps official attributed the exclusions to ongoing changes to Marine Corps systems

⁶Committee on National Security Systems Instruction (CNSSI) No. 1253, *Security Categorization and Control Selection for National Security Systems* (Mar. 27, 2014).

that are designated as CUI systems. As a result, we were able to assess only the Marine Corps based on 89 percent of the required controls.

To assess the reliability of data obtained from eMASS and the Marine Corps Compliance and Authorization Support Tool, we interviewed knowledgeable officials from DOD CIO's eMASS team and the Marine Corps about the quality control procedures used to ensure the accuracy and completeness of the data. We found that the security control data we examined were sufficiently reliable for describing how DOD components implemented CUI security controls.

For objective two, we obtained and analyzed documents used by DOD CIO officials to monitor the components' progress to comply with the CUI requirements identified in their section 1742 report.

To determine the actions that the CIO has taken to address the cybersecurity of CUI systems, we interviewed DOD CIO Office officials about their efforts to address the cybersecurity of CUI systems, and we reviewed relevant DOD cybersecurity policies and guidance. Additionally, we obtained and analyzed documentation related to DOD's efforts to monitor the implementation of these cybersecurity policies and guidance.

We conducted this performance audit from May 2021 to May 2022 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.

Appendix II: Comments from the Department of Defense

**Appendix II: Comments from the Department
of Defense**



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE
8000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

APR 28 2022

Mr. Joseph Kirschbaum
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Kirschbaum:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-22-105259, "Protecting Controlled Unclassified Information (CUI) Systems," May 2022 (GAO Code 105259). Thank you for the opportunity to review and comment on the draft report. The DoD appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing the report.

The Department is pleased to note GAO's extensive review and acknowledgement of the DoD Chief Information Officer's efforts to strive for security compliance within the Department's CUI systems. As noted within the report, the Department has taken action to work with DoD Components to ensure implementation of the appropriate security measures for CUI systems.

The report did not contain any recommendations requiring a response. However, technical comments are under a separate cover.

Again, thank you for the opportunity to review and comment on this report. My point of contact for this matter is Mr. Kevin Dulany, kevin.m.dulany.civ@mail.mil, (571) 372-4699. We look forward to working with you in the future.

Sincerely,

A handwritten signature in blue ink, appearing to read "John B. Sherman".

John B. Sherman

Accessible Text for Appendix II: Comments from the Department of Defense

APR 29 2022

Mr. Joseph Kirschbaum
Director, Information Technology and Cybersecurity
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Kirschbaum:

This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-22-105259, "Protecting Controlled Unclassified Information (CUI) Systems," May 2022 (GAO Code 105259). Thank you for the opportunity to review and comment on the draft report. The DoD appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing the report.

The Department is pleased to note GAO's extensive review and acknowledgement of the DoD Chief Information Officer's efforts to strive for security compliance within the Department's CUI systems. As noted within the report, the Department has taken action to work with DoD Components to ensure implementation of the appropriate security measures for CUI systems.

The report did not contain any recommendations requiring a response. However, technical comments are under a separate cover.

Again, thank you for the opportunity to review and comment on this report. My point of contact for this matter is Mr. Kevin Dulany, kevin.m.dulany.civ@mail.mil, (571) 372-4699. We look forward to working with you in the future.

Sincerely,

John B. Sherman

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Joseph W. Kirschbaum at (202) 512-9971 or KirschbaumJ@gao.gov

Jennifer R. Franks at (404) 679-1831 or at FranksJ@gao.gov

Staff Acknowledgments

In addition to the contacts named above Tommy Baril and Larry Crosland (Assistant Directors), Ashley Houston (Analyst-in-Charge), Mallory Bryan, Vijay D'Souza, and Edward Varty made key contributions to this report. Also, Hiwotte Amare, Tracy Barnes, Christopher Gezon, Richard Powelson, Andrew Stavisky, Khristi Wilkins, and Emily Wilson provided assistance.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

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

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

Congressional Relations

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

Public Affairs

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

Strategic Planning and External Liaison

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



Please Print on Recycled Paper.