

# 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](mailto:kirschbaumj@gao.gov) or (202) 512-9971 or Jennifer R. Franks at [franksj@gao.gov](mailto: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
<b>Categorize DOD CUI systems accurately</b>	No	 80% to 89%
<b>Implement Cybersecurity Maturity Model Certification's 110 security requirements</b>	No	 70% to 79%
<b>Implement 266 security controls for moderate confidentiality impact systems</b>	No <sup>a</sup>	 80% to 89%
<b>Authorize system to operate on DOD network</b>	No	 90% or more

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

<sup>a</sup>DOD 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.