



August 2017

DEFENSE CYBERSECURITY

DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened

Why GAO Did This Study

DOD acknowledges that malicious cyber intrusions of its networks have negatively affected its information technology systems, and that adversaries are gaining capability over time. In 2010, the President re-designated the director of the NSA as CYBERCOM's commander, establishing a dual-hat leadership arrangement for these agencies with critical cybersecurity responsibilities.

House Reports 114-537 and 114-573 both included provisions for GAO to assess DOD's management of its cybersecurity enterprise. This report, among other things, examines (1) DOD officials' perspectives on the advantages and disadvantages of the dual-hat leadership arrangement of NSA/CSS and CYBERCOM, and actions that could mitigate risks if the leadership arrangement ends, and (2) the extent to which DOD has implemented key strategic cybersecurity guidance. GAO analyzed DOD cybersecurity strategies, guidance, and information and interviewed cognizant DOD officials.

What GAO Recommends

GAO recommends that DOD take the following two actions: (1) modify its criteria for closing tasks from *The DOD Cyber Strategy*; and (2) establish a timeframe and monitoring for implementing an objective of the *DOD Cybersecurity Campaign* to transition to commander-driven operational risk assessments for cybersecurity readiness. DOD partially concurred with these recommendations and identified actions it plans to take. If implemented, GAO believes these actions would satisfy the intent of the recommendations.

View [GAO-17-512](#). For more information, contact Joseph W. Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov.

DEFENSE CYBERSECURITY

DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened

What GAO Found

Officials from Department of Defense (DOD) components identified advantages and disadvantages of the "dual-hat" leadership of the National Security Agency (NSA)/Central Security Service (CSS) and Cyber Command (CYBERCOM) (see table). Also, DOD and congressional committees have identified actions that could mitigate risks associated with ending the dual-hat leadership arrangement, such as formalizing agreements between NSA/CSS and CYBERCOM to ensure continued collaboration, and developing a persistent cyber training environment to provide a realistic, on-demand training capability. As of April 2017, DOD had not determined whether it would end the dual-hat leadership arrangement.

Table: Advantages and Disadvantages of the Dual-Hat Leadership Arrangement, as Reported by Department of Defense (DOD) Officials

Advantages	Disadvantages
Improved coordination and collaboration between NSA/CSS and CYBERCOM	Concern that Cyber Command (CYBERCOM) priorities may receive preference over other commands' priorities with respect to National Security Agency (NSA)/Central Security Service (CSS) support
Faster decision-making	Increased potential of NSA/CSS operations and tools being exposed
Efficiency of resources	Too broad of a span of control that potentially limits effective leadership Increases tension between NSA/CSS and CYBERCOM staff who are responsible for military and/or intelligence operation tasks that are not always mutually achievable Enables sharing of resources between NSA/CSS and CYBERCOM resulting in resource allocation that is not always easily understood by personnel

Source: GAO analysis of DOD information. | GAO-17-512

DOD's progress in implementing key cybersecurity guidance—the *DOD Cloud Computing Strategy*, *The DOD Cyber Strategy*, and the *DOD Cybersecurity Campaign*—has varied. DOD has implemented the cybersecurity elements of the *DOD Cloud Computing Strategy* and has made progress in implementing *The DOD Cyber Strategy* and *DOD Cybersecurity Campaign*. However, DOD's process for monitoring implementation of *The DOD Cyber Strategy* has resulted in the closure of tasks before they were fully implemented; for example, DOD closed a task that, among other things, would require completing cyber risk assessments on 136 weapon systems. Officials acknowledged they are on track to complete the assessments by December 31, 2019, but as of May 2017, the task was not complete. Unless DOD modifies its process for deciding whether a task identified in its *Cyber Strategy* is implemented, it may not be able to achieve outcomes articulated in the strategy. Also, DOD lacks a timeframe and process for monitoring implementation of the *DOD Cybersecurity Campaign* objective to transition to commander-driven operational risk assessments for cybersecurity readiness. Unless DOD improves the monitoring of its key cyber strategies, it is unknown when DOD will achieve cybersecurity compliance.

Contents

Letter		1
	Background	6
	Advantages and Disadvantages of the Dual-Hat Arrangement, and Actions That Could Mitigate Potential Risks Associated with Ending the Arrangement	11
	DOD's Implementation of Key Strategic Cybersecurity Guidance Reflects Varied Progress	17
	DOD Has Implemented Fifteen of Twenty-seven Cybersecurity Recommendations from Prior GAO Reports	27
	Conclusions	32
	Recommendations for Executive Action	32
	Agency Comments and Our Evaluation	32
Appendix I	Status of Cybersecurity Recommendations Made to the Department of Defense (DOD), Fiscal Years 2011 through 2016	36
Appendix II	Comments from the Department of Defense	39
Appendix III	GAO Contact and Staff Acknowledgments	40
Related Unclassified GAO Products		41
Tables		
	Table 1: Roles and Responsibilities for the Dual-Hatted Leader of the National Security Agency (NSA)/Central Security Service (CSS) and U.S. Cyber Command (CYBERCOM)	7
	Table 2: Key Roles and Responsibilities for Cybersecurity in the Department of Defense (DOD)	9
	Table 3: Key Department of Defense (DOD) Cybersecurity Strategic Guidance	11
	Table 4: Department of Defense Officials' Perspectives on the Advantages and Disadvantages of the Dual-Hat Leadership Arrangement for the National Security Agency (NSA)/Central Security Service (CSS) and U.S. Cyber Command (CYBERCOM)	12

Table 5: Actions That Could Mitigate Risks Associated with Ending the Dual-Hat, as Identified by National Security Agency (NSA) /Central Security Service (CSS), U.S. Cyber Command (CYBERCOM), and Joint Staff Officials	15
Table 6: Status of Department of Defense Cloud Computing Strategy Cybersecurity Objectives, as of March 2017	18
Table 7: Our Assessment of the Implementation Status of Department of Defense (DOD) Cybersecurity Campaign Objectives, as of March 2017	23
Table 8: Status of GAO Cybersecurity Recommendations by Report, Fiscal Years 2011 through 2016, as of January 2017	27
Table 9: GAO Cybersecurity and High-Priority Cyberspace Recommendations, Fiscal Years 2011 through 2016	36

Figure

Figure 1: Organizational Chart of the Leadership Arrangement for the National Security Agency, Central Security Service, and U.S. Cyber Command	8
---	---

Abbreviations

CIO	Chief Information Officer
CSS	Central Security Service
CYBERCOM	U.S. Cyber Command
DOD	Department of Defense
FOUO	For Official Use Only
NSA	National Security Agency

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.



August 1, 2017

Congressional Committees

The Department of Defense (DOD) faces tens of millions of attempted malicious cyber intrusions per year as adversaries seek to take advantage of the department's reliance upon computer networks. Although only a small fraction of these attempts are successful, any successful intrusion has the potential to provide adversaries with the ability to collect valuable intelligence about capabilities and operations, degrade networks, and manipulate information that commanders need to make timely and critical decisions. In the past decade there have been several high-profile breaches of DOD's information and networks. For example, in 2008, DOD suffered a significant compromise of its networks when a flash drive infected with malicious computer code was inserted into a DOD-owned laptop in the Middle East.¹ The malicious code spread throughout DOD's unclassified and classified networks and enabled data to be transferred to servers under foreign control.

In the past decade, DOD has acknowledged the increasing scope and capability of adversaries to negatively affect DOD information and networks. As such, DOD has taken a number of steps to defend its use of cyberspace from evolving cyber threats. For example, in 2009, DOD established U.S. Cyber Command (CYBERCOM) to, among other things, address the risk of cyber threats and vulnerabilities. In the process of standing up CYBERCOM, in 2010 the President re-designated the Director National Security Agency (NSA) as CYBERCOM's commander, establishing a "dual-hat" leadership arrangement with the intent of allowing CYBERCOM to leverage the existing capabilities and capacity of NSA.² NSA, among other things, serves as the government lead for cryptology, exercises operational control of signals intelligence, and provides cybersecurity products and services in support of DOD. The Director of NSA also serves as the chief of DOD's Central Security Service (CSS), which promotes coordination between NSA and the military service cryptologic elements. Officials told us that NSA and CSS

¹Deputy Secretary of Defense William Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, (Sept./Oct. 2010).

²Secretary of Defense Memorandum, *Establishment of a Subordinate Unified U.S. Cyber Command under U.S. Strategic Command for Military Cyberspace Operations* (June 23, 2009).

are separate organizations, but they now essentially operate as a single entity (henceforth referred to as “NSA/CSS” in this report).

From fiscal years 2011 through 2016, we issued a number of reports on DOD’s efforts to protect against cyberspace threats in which we highlighted management weaknesses across the department and made recommendations that could improve the department’s cyberspace management and operations. In 2015 and 2016, we issued reports in which we emphasized the importance of the recommendations contained in three cybersecurity reports as high-priorities for DOD to address. These reports related to the security of DOD’s defense industrial base, resiliency planning in the event of a cyberattack, and roles and responsibilities for supporting civil authorities in the event of a cyberattack that affects the homeland. Later in this report we discuss these reviews and DOD’s progress in implementing our recommendations in more depth.

House Report 114-537 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2017 and House Report 114-573 accompanying a bill for the Intelligence Authorization Act of Fiscal Year 2017 include provisions for us to assess DOD’s management of progress in protecting its cyber networks, systems, and information—generally equivalent to assessing DOD’s cybersecurity efforts.³ Specifically, DOD defines cybersecurity as the prevention of damage to, protection of, and restoration of computers, electronic communications systems and services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.⁴ This report examines (1) DOD officials’ perspectives on the advantages and disadvantages of maintaining the dual-hat leadership arrangement of NSA/CSS and CYBERCOM, and actions that could mitigate risks entailed in ending the leadership arrangement; (2) the extent to which DOD has implemented key strategic cybersecurity guidance; and (3) the status of DOD’s efforts to implement our cybersecurity recommendations.

To determine DOD officials’ perspectives on the advantages and disadvantages of maintaining the dual-hat leadership arrangement of NSA/CSS and CYBERCOM as well as actions that could mitigate risks

³See H.R. Rep. No. 114-537, at 283-284 (2016) and H.R. Rep. No. 114-573, at 18 (2016).

⁴Department of Defense Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014).

entailed in ending the leadership arrangement, we reviewed documents used by the Joint Staff and CYBERCOM to brief their leadership on the advantages and disadvantages of the arrangement.⁵ We also interviewed officials from NSA/CSS, CYBERCOM, and the office of DOD's Chief Information Officer (CIO) about their perspectives on the advantages and disadvantages of the dual-hat leadership arrangement. Further, we sent a written questionnaire to 25 DOD components, including 9 combatant commands, all 4 military services, 5 combat support agencies, and 7 DOD components responsible for implementing key strategic cybersecurity guidance. The questionnaire contained 10 questions on how the dual-hat leadership arrangement affects cyber missions, functions, and operations, and it instructed recipients to develop responses representing the perspectives of their components. We received 14 complete responses to the dual-hat leadership portion of our questionnaire from CYBERCOM, 6 combatant commands, 4 combat support agencies, and 3 offices within the Office of the Secretary of Defense. We received partial responses from 9 other DOD components, which provided background information on the dual-hat, but not their views on the advantages, disadvantages, and actions to mitigate risks. We did not receive any responses from 2 of the components. DOD CIO also compiled an official response from DOD to the dual-hat leadership arrangement questions that reflected views from across the 25 DOD components to whom we sent questionnaires.

Our report reflects the DOD-wide response and the information we received from the 14 components who responded to our questions. Additionally, we gathered information from NSA/CSS, CYBERCOM, the Joint Staff, components from within the Office of the Secretary of Defense, and the 14 components who responded to our questionnaire on aspects of the dual-hat leadership arrangement between NSA/CSS and CYBERCOM that should be preserved or enhanced, and considerations that should be made before the dual-hat leadership of the organizations is ended. After compiling the documentary evidence, interview results, and questionnaire responses, we grouped the resulting advantages and disadvantages into categories and sent the results with descriptions and examples to officials at NSA/CSS, CYBERCOM, and DOD CIO for review to provide additional assurance that the team accurately and

⁵In a technical comment from DOD, the office of the Principal Cyber Advisor told us that it would consider such actions as "considerations"; however, since considerations cannot mitigate risks, we characterize these efforts as "actions that could mitigate risks" in this report.

appropriately described and categorized the responses. The components provided us with technical comments that we incorporated into the report, as appropriate.

To evaluate the extent to which DOD has implemented key strategic cybersecurity guidance, we first identified DOD's key strategic cybersecurity guidance by asking senior officials from the offices of the Assistant Secretary of Defense for Cyber Policy, the DOD Principal Cyber Advisor, and the DOD CIO to identify the strategies, plans, and guidance currently used by the department to support the implementation of its cybersecurity capabilities. We also sent questionnaires to 25 DOD components instructing them to develop responses representing the perspectives of their components. The questionnaire contained 10 questions on key cyber guidance, and we received responses from 22 of the components for these questions. Based on input provided by senior DOD officials and the responses from the 22 DOD components who responded to our questionnaire, we identified the following three key strategic cybersecurity documents to review: the 2012 *DOD Cloud Computing Strategy*, the 2015 *DOD Cybersecurity Campaign*, and *The DOD Cyber Strategy*, published in 2015.⁶

Second, we reviewed the documents we identified through input from senior DOD officials and responses to our questionnaire in order to gain an understanding of the department's priorities and efforts to defend itself from evolving cyberspace threats. Although the 2012 *DOD Cloud Computing Strategy* and *The DOD Cyber Strategy* focus on a number of cyberspace issues, we limited our review of these documents to the portions related specifically to DOD's *cybersecurity* mission. For example, *The DOD Cyber Strategy* includes five strategic goals focused on cyber operations, cybersecurity, and international cooperation, among other things. To accomplish these goals, DOD identified 49 tasks to complete. For our review, however, we focused on the 22 tasks related specifically to the cybersecurity goal.

Third, we collected tracking information and planning documents on DOD's cybersecurity efforts in order to learn about the internal controls for, and determine the extent to which, the department reported

⁶Department of Defense Chief Information Officer, *Cloud Computing Strategy* (July 2012); Department of Defense, *DOD Cybersecurity Campaign* (June 2015)(FOUO); and Department of Defense, *The Department of Defense Cyber Strategy* (April 2015) (hereinafter cited as *The DOD Cyber Strategy*).

implementing the specific goals, objectives, or tasks associated with the key strategic cybersecurity guidance. Documents we obtained included monthly implementation status updates from the Principal Cyber Advisor on the tasks related to *The DOD Cyber Strategy*, and DOD's Cybersecurity Scorecard, which monitors key tasks from the four lines of effort in the *DOD Cybersecurity Discipline Implementation Plan*. We compared the internal control activities established in these documents with the monitoring standards established in the Office of Management and Budget's *Management Responsibility for Enterprise Risk Management and Internal Control* and the *Standards for Internal Control in the Federal Government*.⁷ In addition, we discussed the department's plans and implementation status with DOD officials within the component organizations primarily responsible for implementing the key strategic cybersecurity guidance in order to determine the extent to which the efforts were implemented and closed and to learn more about the internal control environment. Specifically, we met with DOD officials from the offices of the DOD Principal Cyber Advisor; DOD CIO; Under Secretary of Defense for Policy; and Under Secretary of Defense for Acquisitions, Technology, and Logistics. We also met with officials from the Joint Staff; CYBERCOM, and the Defense Information Systems Agency. Finally, for the efforts DOD reported as implemented, we compared documentary evidence of the department's actions with the relevant cybersecurity requirement to determine whether the actions satisfied the goal, objective, or task identified in the key strategic cybersecurity guidance. However, we did not test the effectiveness of DOD's implementation. For those efforts DOD reported as in progress, we discussed the implementation status and the challenges, if any, that might impede implementation.

To determine the status of DOD's efforts to implement our cybersecurity recommendations, we reviewed the implementation status of cybersecurity recommendations made to DOD from fiscal years 2011 through 2016. For the purposes of this report, we focused our efforts on our reports that included cybersecurity-related recommendations to DOD. Once we identified the reports to include in our review, we used our recommendation tracking system to determine the status of the recommendations—i.e., open, closed as implemented, or closed as not-implemented. Open recommendations represent those that DOD is still

⁷Office of Management and Budget, Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (Washington, D.C.: Jul. 15, 2016); and GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

taking actions to implement. For those recommendations that were listed as open, we coordinated with DOD officials responsible for implementing the recommendations to identify any actions DOD has taken to do so. Where DOD has taken actions, we determined whether the actions taken and documents DOD has provided would enable us to change the status of the recommendation.

We conducted this performance audit from June 2016 to August 2017 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.

Background

DOD's Use of Dual-Hatting “Dual-hatting” is a term used to describe a position in which an incumbent officer has responsibilities in two organizations simultaneously—usually to that officer’s particular military service, and to a joint, combined, or international organization or activity.⁸ DOD officials told us that dual-hatting senior leaders is a relatively common practice within DOD to help align authorities, improve mission effectiveness, and use a senior leader’s experience and expertise while balancing the scope of responsibility. Some prominent examples of dual-hatting include the Commander of U.S. Northern Command also serving as the Commander of the North American Aerospace Defense Command; and the Commander of U.S. European Command also serving as the Supreme Allied Commander Europe (that is, the commander of military operations conducted by the North Atlantic Treaty Organization). Additionally, the Air Force and Navy commanders who support U.S. European Command are dual-hatted as service component commanders for U.S. Africa Command.

⁸Chairman of the Joint Chiefs of Staff Instruction 1330.05A, *Joint Officer Management Program Procedures*, Enclosure D (Dec. 15, 2015).

The Dual-Hat Leadership of NSA/CSS and CYBERCOM

When the Secretary of Defense directed CYBERCOM's establishment in 2009, he also recommended to the President that the position of Director of NSA be assigned the responsibility for leading this new command. DOD officials told us the dual-hat leadership arrangement originated to allow CYBERCOM to use NSA/CSS infrastructure and tools to carry out its mission more quickly and to establish unity of command and effort for DOD in the cyberspace domain. As the sole leader of these organizations, the dual-hatted leader is responsible for a broad set of roles and responsibilities, as outlined below in table 1.

Table 1: Roles and Responsibilities for the Dual-Hatted Leader of the National Security Agency (NSA)/Central Security Service (CSS) and U.S. Cyber Command (CYBERCOM)

Position	Roles and Responsibilities
Director of NSA ^a	<ul style="list-style-type: none"> U.S. government lead for cryptology principal advisor to the Department of Defense (DOD) on signals intelligence exercises signals intelligence operational control and establishes policies and procedures for departments and agencies to follow to appropriately, effectively, and efficiently perform signals intelligence provides information assurance guidance and assistance to DOD and national customers develops and manages the NSA portion of the Military Intelligence Program resources and capabilities
Chief of CSS ^a	<ul style="list-style-type: none"> promotes full partnership between NSA and the cryptologic elements of the Armed Forces in the execution of signals intelligence and other cryptologic operations
Commander of CYBERCOM ^b	<ul style="list-style-type: none"> defends critical cyberspace assets, systems, and functions against intrusion or attack^c secures, operates, and defends the DOD information network^c synchronizes and directs transregional cyberspace operations in coordination with other combatant commands, the Joint Staff, and the Office of the Secretary of Defense, liaises with other U.S. government departments and agencies, and members of the defense industrial base in conjunction with the Department of Homeland Security. conducts full spectrum military cyberspace operations in order to ensure freedom of action in cyberspace and deny the same to adversaries

Source: GAO analysis of DOD information. | GAO-17-512

^aDepartment of Defense Directive 5100.20, *National Security Agency/Central Security Service (NSA/CSS)* (Jan. 26, 2010).

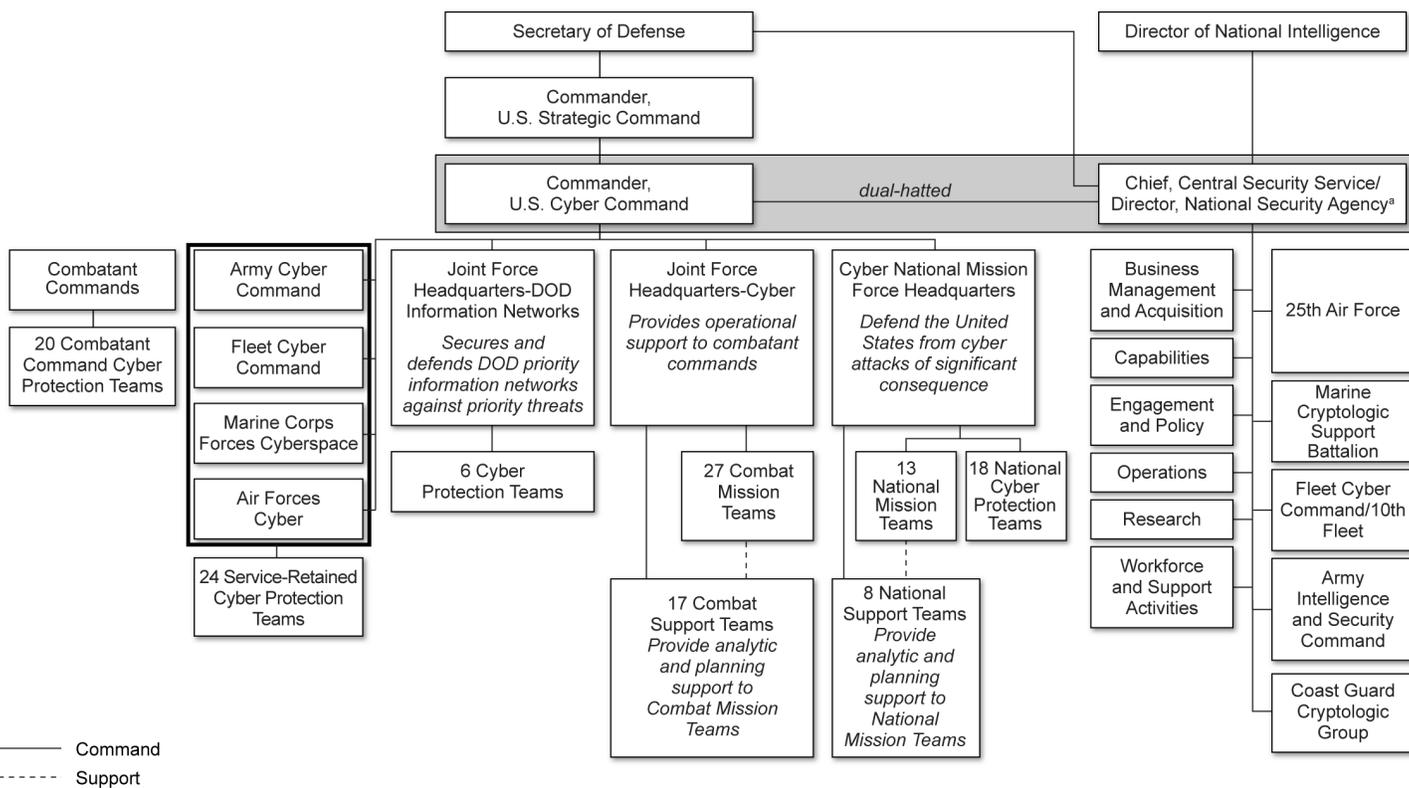
^bDerived from Joint Publication 3-12(R), *Cyberspace Operations* (Feb. 3, 2013) and U.S. Strategic Command's website on U.S. Cyber Command.

^cCommander of United States Strategic Command has overall responsibility for operating the DOD information network, but performs these functions through a subunified command, CYBERCOM. See Joint Publication 3-12(R), *Cyberspace Operations* (Feb. 3, 2013).

Since its establishment, CYBERCOM has operated as a sub-unified command organized under U.S. Strategic Command, and this arrangement continues as of April 2017. The National Defense Authorization Act for Fiscal Year 2017 included a provision directing the

President to establish CYBERCOM as a unified combatant command.⁹ When the President and DOD implement this provision, CYBERCOM will no longer be organized under U.S. Strategic Command. Figure 1 below depicts the NSA/CSS and CYBERCOM leadership arrangement, as of April 2017, and where those offices fit within DOD's organization. The figure also provides an overview of CYBERCOM's 133 Cyber Mission Force Teams, which carry out particular parts of CYBERCOM's mission.

Figure 1: Organizational Chart of the Leadership Arrangement for the National Security Agency, Central Security Service, and U.S. Cyber Command



Source: GAO analysis of Department of Defense (DOD) information. | GAO-17-512

^aIn addition to being a member of the intelligence community that focuses on national-level intelligence priorities, the National Security Agency/Central Security Service is also a Combat Support Agency—a component of DOD—that addresses military intelligence priorities and provides information assurance support to the military.

⁹See Pub. L. No. 114-328, § 923 (2016).

As CYBERCOM has matured, leaders—including Congress, the President, the Director of National Intelligence, and the current leader of NSA/CSS and CYBERCOM—have discussed the concept of ending the dual-hat leadership of the two organizations, such that one individual would lead NSA/CSS and another individual would lead CYBERCOM. Section 1642 of the National Defense Authorization Act for Fiscal Year 2017 enumerated a number of conditions that the Secretary of Defense and the Chairman of the Joint Chiefs of Staff must jointly certify before the dual-hat leadership arrangement for NSA and CYBERCOM can be terminated.¹⁰ While DOD officials have considered ending the dual-hat leadership arrangement, as of April 2017, the department has not decided whether to do so.

DOD Components with Cybersecurity Responsibilities

To establish a cybersecurity program to protect and defend DOD information and information technology, DOD has assigned some of its components and senior officials with cybersecurity responsibilities, summarized in table 2 below.

Table 2: Key Roles and Responsibilities for Cybersecurity in the Department of Defense (DOD)

DOD Senior Officials and Components	Key Cybersecurity Roles and Responsibilities
Principal Cyber Advisor	Principal advisor to the Secretary of Defense on cyber-related activities, including policy and operational considerations, resources, personnel, acquisition, and technology. Oversees implementation of <i>The DOD Cyber Strategy</i> and other relevant policy and planning documents to help achieve DOD’s Cyber mission, goals, and objectives.
DOD Chief Information Officer (CIO)	Principal staff assistant and senior advisor to the Secretary of Defense for information technology, information resources management, and efficiencies. Oversees management of DOD cyberspace information technology and cybersecurity workforce. Monitors, evaluates, and provides advice to the Secretary of Defense regarding all DOD cybersecurity activities. Coordinates with the National Institute of Standards and Technology in development of cybersecurity-related standards and guidelines. Responsible for policy, oversight, and guidance for the architecture and programs related to DOD’s networking and cyber defense.
Under Secretary of Defense for Acquisitions, Technology, and Logistics ^a	Oversees all DOD cyber-capability acquisitions; establishes the architecture for a DOD enterprise-wide interoperability test capability; oversees DOD cybersecurity research and engineering investments, including research at the National Security Agency; ensures information assurance training of the DOD acquisition workforce; oversees relevant defense contract regulations.

¹⁰See Pub. L. No. 114-328, § 1642 (2016).

DOD Senior Officials and Components	Key Cybersecurity Roles and Responsibilities
Under Secretary of Defense for Policy	Serves as the principal staff assistant and advisor to the Secretary of Defense for all matters on the formulation of national security and defense policy and the integration and oversight of DOD policy and plans to achieve national security objectives. Coordinates with DOD CIO to ensure that cybersecurity strategies, policies, and capabilities are aligned with overarching DOD cyberspace policy; develops and implements international cyberspace strategies and policies; and enhances DOD's and the defense industrial base's situational awareness of cyber threats.
Under Secretary of Defense for Intelligence	Serves as principal staff assistant and advisor to the Secretary of Defense regarding intelligence, counterintelligence, security, sensitive activities, and other intelligence-related matters. Coordinates with DOD CIO on the development and implementation of cybersecurity policy, guidance, procedures, and controls related to personnel, physical, industrial, information, and operations security. Ensures the development of balanced intelligence support to the cyberspace operations portfolio that is integrated with the activities of the DOD components and interagency and allied partners. Coordinates future research and strategic assessments to inform investments for long-range planning and implementation of intelligence capabilities and capacity supporting cyberspace operations.
Under Secretary of Defense for Personnel and Readiness	Serves as the principal staff assistant and advisor for total force management, including readiness and training, and military and civilian personnel requirements. Supports implementation of cybersecurity requirements for effective manning, management, and readiness assessment of the cybersecurity workforce.
National Security Agency/Central Security Service	Provides support to DOD components for assessing threats to, and vulnerabilities of, information technologies, and provides cybersecurity products and services in support of DOD components' military, intelligence, and business functions.
U.S. Cyber Command	Provides mission assurance for the operation and defense of the DOD information environment, defends the nation against strategic threats to U.S. interests and infrastructure, and supports the achievement of joint force commander objectives.
Defense Information Systems Agency	Provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national-level leaders, and other mission and coalition partners across the full spectrum of operations.

Source: GAO analysis of DOD information. | GAO-17-512

Note: These DOD components and senior officials have a number of roles and responsibilities that are identified in DOD directives, instructions, memorandums, and guidance documents. For the purposes of this table we focused only on these components' cybersecurity roles and responsibilities.

^aSection 901 of the National Defense Authorization Act for Fiscal Year 2017 directs the reorganization of the position of Under Secretary of Defense for Acquisition, Technology, and Logistics by February 2018 into two separate Under Secretaries of Defense: an Under Secretary of Defense for Research and Engineering and an Under Secretary of Defense for Acquisition and Sustainment.

Key DOD Strategic Cybersecurity Guidance	DOD has issued guidance to support the implementation of its cybersecurity capabilities. Table 3 below lists key DOD strategic-level cybersecurity documents and includes a description of each document, as well as the component organization(s) primarily responsible for their implementation.
--	--

Table 3: Key Department of Defense (DOD) Cybersecurity Strategic Guidance

Document	Description	Organization(s) Primarily Responsible for Implementation
<i>The DOD Cyber Strategy</i> , issued in 2015	Guides the development of DOD’s cyber forces and strengthens cyber defense and deterrence. Defines three primary cyberspace missions for DOD: (1) defend DOD networks, systems, and information; (2) be prepared to defend the United States and its interests against cyberattacks of significant consequence; and (3) provide cyber capabilities to support military operations and contingency plans.	Office of the DOD Principal Cyber Advisor; Office of the DOD Chief Information Officer (CIO); Office of the Under Secretary of Defense for Policy; Office of the Under Secretary of Defense for Acquisitions, Technology, and Logistics; Under Secretary of Defense for Intelligence; the Joint Staff; U.S. Cyber Command
2015 <i>DOD Cybersecurity Campaign</i> (FOUO)	Identifies seven actions to drive commanders and senior leaders to enforce full cybersecurity compliance and accountability across the department. The <i>DOD Cybersecurity Scorecard</i> and <i>DOD Cybersecurity Discipline Implementation Plan</i> are two sub-efforts of this campaign ^a	Office of the DOD CIO; Office of the Under Secretary of Defense for Acquisitions, Technology, and Logistics; U.S. Cyber Command; Defense Information Systems Agency
2012 <i>DOD Cloud Computing Strategy</i>	Identifies ways for DOD to take advantage of cloud computing to accelerate the delivery, efficiency, and innovation of information technology.	DOD CIO

Source: GAO analysis of DOD information. | GAO-17-512

^aThe purpose of the *DOD Cybersecurity Discipline Implementation Plan* is to direct commanders and supervisors to implement strong authentication, device hardening, and other actions to mitigate risks and operationalize cyber readiness reporting for the information systems they own, manage, or lease for mission assurance through the Defense Readiness Reporting System. The Cybersecurity Scorecard is designed to provide senior DOD leaders with data to monitor the highest priority items in the *DOD Cybersecurity Discipline Implementation Plan*.

Advantages and Disadvantages of the Dual-Hat Arrangement, and Actions That Could Mitigate Potential Risks Associated with Ending the Arrangement

Officials from various DOD components identified advantages and disadvantages of the dual-hat leadership of NSA/CSS and CYBERCOM. Additionally, DOD and Congress have identified actions that could mitigate the risks associated with ending the dual-hat leadership arrangement. As of March 2017, DOD officials informed us that DOD had not determined whether it would end the dual-hat leadership arrangement and was reviewing the steps and funding necessary to meet the requirements established in the law.

Advantages and Disadvantages of the Dual-Hat Leadership Arrangement

According to officials, DOD does not have an official position on the advantages and disadvantages of the dual-hat leadership arrangement of NSA/CSS and CYBERCOM. Through responses to interviews and questionnaires, officials from DOD components provided their perspectives on the advantages and disadvantages associated with the dual-hat leadership arrangement as summarized in table 4, below.

Table 4: Department of Defense Officials' Perspectives on the Advantages and Disadvantages of the Dual-Hat Leadership Arrangement for the National Security Agency (NSA)/Central Security Service (CSS) and U.S. Cyber Command (CYBERCOM)

Advantage or Disadvantage	Description
Advantages	
More in-depth coordination and collaboration	Officials from several DOD components reported that the dual-hat allows senior leaders from each organization to have visibility into each organization's processes and procedures. This has led to the development of internal processes that encourage coordination and collaboration between appropriate personnel and allow for coordinated efforts on capability development, testing, and business processes. In the absence of the dual-hat, NSA/CSS and CYBERCOM would need to formalize these internal processes in order to maintain them.
Faster decision-making	Officials from several DOD components, including NSA/CSS and CYBERCOM, reported that the dual-hat enables both organizations to elevate issues and receive a final decision from a single leader, instead of elevating issues up two separate chains of command to build consensus across commands. Specifically, the arrangement can allow for decisions to be made without taking issues to the Secretary of Defense and/or Director of National Intelligence for resolution, which could be necessary if separate leaders of NSA/CSS and CYBERCOM disagreed on an issue.
More efficient use of resources	Officials from several DOD components, including NSA/CSS and CYBERCOM, reported that the dual-hat allows NSA/CSS and CYBERCOM to share, within authorized, well-defined and mutually agreed-upon parameters, cyber and physical infrastructure, as well as develop and host combined training and training standards in accordance with established inter-service support agreements and memorandums of understanding.
Disadvantages	
Concerns about unfair prioritization of requests for support	Officials from CYBERCOM reported learning of other commands' concerns that CYBERCOM priorities may receive preference over other commands' priorities with respect to NSA/CSS support, should the dual-hat leadership arrangement continue, particularly when CYBERCOM attains the authorities of a unified combatant command. ^a
Increased potential for exposure of NSA/CSS tools and operations	The dual-hat command structure has led to a high level of CYBERCOM dependence on NSA/CSS tools and infrastructure. According to NSA/CSS officials, the agency shares its tools and tactics for gaining access to networks with a number of U.S. government agencies, but CYBERCOM's dependence on and use of the tools and accesses is particularly prevalent. CYBERCOM's dependence on NSA/CSS tools increases the potential that the tools could be exposed.
Broad span of control	DOD officials reported that the responsibilities may be too broad for a single individual. For example, NSA/CSS and CYBERCOM officials agreed that as CYBERCOM reaches maturity, the number of operations will likely grow, and the breadth, depth, and magnitude of the issues required to be managed by a single person leading both CYBERCOM and NSA/CSS could be overwhelming.

Advantage or Disadvantage	Description
Tension between military operations and intelligence operations/actions	Officials from NSA/CSS and CYBERCOM, including a senior-level official, reported that—as both the leader of an intelligence agency and commander of a military command—the dual-hat leads to increased tension between NSA/CSS staff and CYBERCOM staff. Specifically, while CYBERCOM is primarily focused on conducting military operations in cyberspace, NSA/CSS is primarily focused on supporting both national and military intelligence priorities in its roles as an intelligence agency and combat support agency. These objectives, especially with respect to a specific mission, may not always be mutually achievable.
Limited understanding of resourcing	DOD officials reported that while the dual-hat allows for mutually beneficial sharing of resources, it results in resource allocation that is not always easily understood by all personnel. Officials from NSA/CSS explained that NSA/CSS uses its resources to acquire and provide capabilities for CYBERCOM. CYBERCOM officials responded that such funding is tracked according to statutory and regulatory requirements. For example, NSA/CSS and U.S. Strategic Command have an inter-service support agreement that details various costs associated with the establishment and operation of CYBERCOM.

Source: GAO analysis of DOD information. | GAO-17-512

^aIn addition to determining when the department should end the dual-hat leadership arrangement, DOD is also in the process of implementing the elevation of U.S. Cyber Command from a sub-unified command to a unified combatant command, as specified in Section 923 of the National Defense Authorization Act for Fiscal Year 2017.

DOD Components and Congress Have Identified Actions That Could Mitigate Potential Risks Associated with Ending the Dual-Hat Leadership Arrangement

Actions Identified by DOD Component Officials to Mitigate Potential Risks Associated with Ending the Dual-Hat Leadership Arrangement

In response to the National Defense Authorization Act for Fiscal Year 2017, President Obama supported elevating CYBERCOM to a unified combatant command and stated that NSA/CSS and CYBERCOM should have separate leaders who are able to devote themselves to each organization’s respective missions and responsibilities, but who should continue to leverage the shared capabilities and synergies developed

under the dual-hat arrangement.¹¹ As of April 2017, DOD officials told us that the department supports elevating CYBERCOM to a unified combatant command, but recognizes that there are potential risks in ending the dual-hat leadership arrangement. Prior to the passage of the National Defense Authorization Act for Fiscal Year 2017, DOD components, such as CYBERCOM and the Joint Staff, had already developed internal lists of conditions and prerequisites that could mitigate risks prior to ending the dual-hat leadership arrangement. These considerations were presented to senior leadership within the respective components to help inform their positions on ending the dual-hat leadership arrangement.

According to DOD officials, discontinuing the dual-hat arrangement would require DOD to put the necessary policies and processes in place to continue the mutually beneficial partnership between NSA/CSS and CYBERCOM. Specifically, the arrangement in conjunction with support agreements has enabled CYBERCOM to leverage the capability development, personnel, facilities, infrastructure, testing capabilities, and business processes of NSA/CSS to support CYBERCOM operations. DOD officials also cited the potential for less communication between CYBERCOM and NSA/CSS and slower decision-making if the leadership arrangement were ended. Table 5 below lists the various actions reported to us by officials from DOD components that could mitigate risks associated with ending the dual-hat command structure of NSA/CSS and CYBERCOM, as well as the status of these actions, as of March 2017. According to DOD officials, many of these factors relate as much to the growth and maturation of CYBERCOM as they do the dual-hat status.

¹¹In Section 1642 of the National Defense Authorization Act for Fiscal Year 2017, Congress mandated that the Secretary of Defense and the Chairman of the Joint Chiefs of Staff must jointly certify, among other things, that the termination of the dual-hat arrangement will not pose risks to the military effectiveness of CYBERCOM that are unacceptable to the national security interests of the United States. Section 1642 also requires DOD to conduct an assessment and specifies several elements of the assessment such as an evaluation of the ability of CYBERCOM and NSA to carry out their respective roles and responsibilities independently, and whether certain conditions have been met before the dual-hat leadership arrangement for NSA and CYBERCOM can be terminated.

Table 5: Actions That Could Mitigate Risks Associated with Ending the Dual-Hat, as Identified by National Security Agency (NSA) /Central Security Service (CSS), U.S. Cyber Command (CYBERCOM), and Joint Staff Officials

Actions That Could Mitigate Risks	Status of Actions (as of March 2017)
Achieve full operational capability for the 133 Cyber Mission Force Teams	Initial operational capability achieved in October 2016, full operational capability planned for no later than September 2018.
Formalize agreements between NSA/CSS and CYBERCOM to ensure collaboration on key issues	NSA/CSS and CYBERCOM have agreements in place to foster collaboration. NSA/CSS and CYBERCOM officials told us there are advantages afforded to both organizations by the dual-hat leadership arrangement that they are working to formalize. Currently an agreement has been drafted, but not approved.
Develop a persistent cyber training environment to provide a realistic, on-demand training capability	DOD continues to develop the persistent cyber training environment, but it is not yet complete.
Develop independent Title 10 cyber capabilities for CYBERCOM that do not rely as much upon NSA/CSS Title 50 infrastructure ^a	In May 2017, the Commander of CYBERCOM testified that splitting the leadership of the organizations would functionally impair mission effectiveness.
Elevate and resource CYBERCOM to a unified combatant command	The National Defense Authorization Act for Fiscal Year 2017 directs the President to establish Cyber Command as a unified combatant command. According to DOD, the department has prepared for potential elevation since 2012 and much preparatory work has already been done, however the decision to elevate the command has not yet been made. The department has included \$50 million in the budget amendment to fund initial elevation requirements and, as of April 2017, was still finalizing future funding needs.
Complete implementation of NSA-21 reorganization initiative	The NSA in the 21 st Century (NSA-21) campaign was launched in February 2016, and is centered around a set of initiatives designed to improve the agency's performance in the areas of people, innovation, and integration, with an organizational realignment to support the implementation of these initiatives. Officials expect this two-year campaign to reach full operational capability in December 2017.

GAO analysis of DOD information. | GAO-17-512

^aTitle 10 of the U.S. Code generally refers to the role of the armed forces to provide for the national defense and to man, train, and equip forces for military operations in cyberspace. Title 50 of the U.S. Code generally refers to a broad range of military, foreign intelligence, and counterintelligence activities to include operations in cyberspace.

Congressional Interest in and Conditions for Ending Dual-Hat

Separate from actions identified by select DOD components, Congress has requested information from the department and required it to meet specific conditions and to certify that the termination of the dual-hat arrangement, if pursued by DOD, will not pose risks to the military effectiveness of CYBERCOM that are unacceptable to the national security interests of the United States. Specifically, House Report 114-537 accompanying a bill for the National Defense Authorization Act of Fiscal Year 2017 and House Report 114-573 accompanying a bill for the Intelligence Authorization Act of Fiscal Year 2017 directed the Secretary of Defense to provide the House defense and intelligence committees with a briefing and an assessment of the dual-hat command by November 1, 2016. According to the committee direction, DOD was to address the following:

-
1. roles and responsibilities, including intelligence authorities, of each organization;
 2. assessment of the current impact of the dual-hat relationship, including both advantages and disadvantages;
 3. recommendations on courses of action for separating the dual-hat command relationship between the Commander of CYBERCOM and the Director of the NSA/Chief of CSS, if appropriate;
 4. suggested timelines for carrying out such courses of action; and
 5. recommendations for legislative actions, as necessary.¹²

DOD did not perform this briefing and assessment. Performing this assessment would have provided DOD with an opportunity to articulate its perspectives on the advantages and disadvantages of the dual-hat leadership arrangement. Further, it would have allowed DOD to present its preferred course of action in relation to separating the leadership of NSA/CSS and CYBERCOM. DOD officials told us that they believed the assessment they were directed to provide to the House defense and intelligence committees in November 2016 was no longer necessary, based on Section 1642 of the National Defense Authorization Act for Fiscal Year 2017. However, while the act did not include the same briefing and assessment requirement identified in the two House reports, the act also did not cancel the committee direction. In addition, the briefing requirement still exists, as evidenced by the explanatory statement accompanying the Intelligence Authorization Act for Fiscal Year 2017, for DOD to brief and provide an assessment of the dual-hat leadership arrangement.¹³

According to Section 1642 of the National Defense Authorization Act for Fiscal Year 2107, DOD cannot terminate the dual-hat leadership arrangement until the Secretary of Defense and the Chairman of the Joint Chiefs of Staff jointly certify that the termination will not pose risks to the military effectiveness of CYBERCOM that are unacceptable to the national security interests of the United States. Section 1642 also requires DOD to conduct an assessment that, among other things, evaluates CYBERCOM's operational dependence on NSA and evaluates each organization's ability to carry out its roles and responsibilities

¹²See H.R. Rep. No. 114-537, at 309-310 (2016) and H.R. Rep. No. 114-573, at 17-18 (2016).

¹³See 163 Cong. Rec. (H3301)(May 3, 2017).

independently. In addition, Section 1642 requires DOD to determine whether the following conditions have been met before deciding to end the dual-hat leadership arrangement:

- Robust operational infrastructure has been deployed that is sufficient to meet the unique cyber mission needs of CYBERCOM and NSA, respectively.
- Robust command and control systems and processes have been established for planning, deconflicting, and executing military cyber operations.
- The tools and weapons used in cyber operations are sufficient for achieving required effects.
- Capabilities have been established to enable intelligence collection and operational preparation of the environment for cyber operations.
- Capabilities have been established to train cyber operations personnel, test cyber capabilities, and rehearse cyber missions.
- The cyber mission force has achieved full operational capability.

Office of the Under Secretary of Defense for Intelligence and Joint Staff officials told us that they regularly discuss matters related to ending the dual-hat leadership arrangement of NSA/CSS and CYBERCOM. However, as of April 2017, DOD's senior leaders had not decided whether the dual-hat leadership should be ended, and the department was reviewing the steps and funding necessary to meet the statutory requirement of Section 1642.

DOD's Implementation of Key Strategic Cybersecurity Guidance Reflects Varied Progress

DOD's implementation of key strategic cybersecurity guidance—the *DOD Cloud Computing Strategy*, *The DOD Cyber Strategy*, and the *DOD Cybersecurity Campaign*—to help manage and focus its cybersecurity efforts has varied. The department has implemented the cybersecurity objectives identified in the *DOD Cloud Computing Strategy*, and it has made progress in implementing *The DOD Cyber Strategy* and *DOD Cybersecurity Campaign*. However, the department's process for monitoring implementation of *The DOD Cyber Strategy* has resulted in the closure of tasks as implemented before the tasks were fully implemented. In addition, the *DOD Cybersecurity Campaign* lacked timeframes for completion and a process to monitor progress, which together provide accountability to ensure implementation.

DOD Has Implemented the Four Cybersecurity Objectives of the 2012 DOD Cloud Computing Strategy

DOD has implemented the four cybersecurity objectives of the 2012 *DOD Cloud Computing Strategy*. In July 2012, the DOD CIO issued the *DOD Cloud Computing Strategy*, which laid the groundwork for accelerating cloud adoption in the department, consistent with the *Federal Cloud Computing Strategy*.¹⁴ The *DOD Cloud Computing Strategy* includes four objectives aimed at enhancing the department's cybersecurity, as listed in table 6 below, along with DOD's status in implementing the objectives.

Table 6: Status of Department of Defense Cloud Computing Strategy Cybersecurity Objectives, as of March 2017

Objective	Status
Leverage efforts such as the Federal Risk and Authorization Management Program that help standardize and streamline certification and accreditation processes for commercial and federal government cloud providers, allowing approved information technology capabilities to be more readily shared across the department.	Implemented
Move from a framework of traditional system-focused certification and accreditation with periodic assessments to continual reauthorization through implementation of continuous monitoring.	Implemented
Move to standardized and simplified identity and access management.	Implemented
Reduce network seams through network and data center consolidation and implementation of a standardized infrastructure.	Implemented

Source: GAO analysis of DOD documentation. | GAO-17-512

In March 2016 DOD issued the *DOD Cloud Computing Security Requirements Guide*, which outlines the security controls and requirements necessary for using cloud-based solutions.¹⁵ According to DOD officials, the *Cloud Computing Security Requirements Guide* is the basis for authorizing commercial cloud service providers in the DOD environment and is closely aligned with the Federal Risk and Authorization Management Program—the fundamental cloud approval process for the federal government. This guide establishes a standardized infrastructure for cloud-based services, continuous monitoring, and identity and access management. According to DOD CIO officials, DOD has approved more than 50 commercial cloud networks for various levels of use based on this guidance. Additionally, in October 2016, DOD finalized the *Defense Federal Acquisition Regulation Supplement* interim rule on network penetration reporting and contracting for cloud services, which further standardized infrastructure requirements

¹⁴Department of Defense Chief Information Officer, *Department of Defense Cloud Computing Strategy* (Washington, D.C.: July 2012); The White House, United States Chief Information Officer. *Federal Cloud Computing Strategy* (Washington, D.C.: Feb. 8, 2011).

¹⁵Defense Information Systems Agency. *DOD Cloud Computing Strategy Security Requirements Guide, Version 1, Release 2* (Mar. 18, 2016).

for cloud service providers.¹⁶ In April 2017, DOD also submitted a Data Center Optimization Strategic Plan, as required by the Office of Management and Budget, which lays out the number of data centers DOD expects to close through fiscal year 2018 as well as estimated cost savings associated with those closures. The plan DOD submitted shows that the department closed more than 150 data centers in fiscal year 2016 and planned to close more over the following 2 years, which would help reduce network seams through network and data center consolidation.

DOD Has Taken Some Actions on All Cybersecurity Tasks Supporting The DOD Cyber Strategy, but the Current Process for Monitoring Implementation Limits Oversight of Tasks to Completion

DOD has taken some actions on all 22 cybersecurity-related tasks identified in *The DOD Cyber Strategy*, although it has closed some tasks before they were fully implemented. The purpose of *The DOD Cyber Strategy*, issued in April 2015, is to guide the development of DOD's cyber forces and strengthen cyber defense and cyber deterrence postures. This strategy, according to DOD, presents an aggressive, specific plan for leaders from across the department to take action and hold their organizations accountable to achieve the strategy's objectives. *The DOD Cyber Strategy* sets prioritized strategic goals and objectives for DOD's cyber activities and missions to achieve over the ensuing five years (that is, through 2020). The Office of the Under Secretary of Defense for Policy; Office of the Principal Cyber Advisor to the Secretary of Defense; the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Joint Staff work with the DOD components to prioritize and oversee the implementation of this strategy and its objectives and to assign responsibility for managing each objective. In a June 2015 memorandum, then Secretary of Defense Ashton Carter identified the implementation of *The DOD Cyber Strategy* as one of his top priorities and stated that the department should ensure that the outcomes articulated in the strategy were achieved.¹⁷

DOD has taken actions on all 22 of the tasks associated with the cybersecurity goal of the strategy that focuses on network defense,

¹⁶Defense Acquisition Regulations System, *Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services*, 81 Fed. Reg. 72986 (Oct. 21, 2016).

¹⁷Secretary of Defense Memorandum, *Designation of Office of Primary Responsibility for Lines of Effort and Objectives in the DOD Cyber Strategy* (June 19, 2015).

mission assurance, and security of the defense industrial base.¹⁸ For example, the Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics and the Office of the Undersecretary of Defense for Intelligence formed a working group—the joint acquisition protection and exploitation cell—that links intelligence, counterintelligence, and law enforcement agents with acquisition program managers to prevent and mitigate data loss and theft. This working group ensures that federal acquisition rules and guidance mature over time in a manner consistent with standards, and it establishes an analysis capability to improve protection of controlled technical information and other critical information department-wide. In another example, DOD has adopted activities that include both regulatory and voluntary programs to improve the cybersecurity of defense industrial base companies. Companies maintaining covered defense information or providing critical support are now contractually required to report cyber incidents and use security standards identified in a National Institute of Standards and Technology special publication on protecting controlled unclassified information in nonfederal information systems.¹⁹ In addition, in October 2015, DOD modified eligibility criteria for participants in the defense industrial base cybersecurity information sharing program.²⁰ Since this revision, DOD officials reported that program participation expanded from 124 to 207 industry partners.

While DOD has taken some actions on all 22 cybersecurity tasks, we found that it has closed some tasks before they were fully implemented. This increases the risk that DOD will not fully implement those tasks, and also increases the risk that leadership will not be aware of delays or complications related to fully implementing *The DOD Cyber Strategy*. Specifically, the Principal Cyber Advisor has closed tasks when that office confirms that the DOD component primarily responsible for implementation has begun taking action on the tasks and follow-on work to complete the tasks has been integrated into existing DOD processes, operations, or policies. For example, DOD closed the task that required

¹⁸*The DOD Cyber Strategy* identified the department's five strategic goals, including one that focuses on the cybersecurity of DOD's information network and systems. According to *The DOD Cyber Strategy* tracking tool, the department has initiated action on all 49 tasks that support the strategy—including the 22 tasks focused specifically on cybersecurity.

¹⁹See Federal Acquisition Regulation (FAR), 48 C.F.R. § 252.204-7012; see also 32 C.F.R. § 236.4.

²⁰See *Defense Acquisition Regulations System: DOD Defense Industrial Base Cybersecurity Activities*, 80 Fed. Reg. 59581 (Oct. 2, 2015); see also 32 C.F.R. § 236.

the department to assess the cybersecurity of current and future weapon systems. According to *The DOD Cyber Strategy*, DOD is to assess and initiate cybersecurity improvements for existing weapon systems; mandate cybersecurity requirements for future weapon systems; and update acquisition and procurement policies to promote effective cybersecurity. The Deputy Principal Cyber Advisor approved closing this task in *The DOD Cyber Strategy* monitoring process when the Under Secretary of Defense for Acquisition, Technology, and Logistics submitted a plan to Congress that was required by a provision in the National Defense Authorization Act for Fiscal Year 2016 and established a process to develop cybersecurity requirements for future weapon systems.²¹ In response to both *The DOD Cyber Strategy* task and the provision in the National Defense Authorization Act for Fiscal Year 2016, DOD—under the leadership of the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics—initiated assessments of its existing weapon systems. In addition to initiating these assessments and establishing a process to develop cybersecurity requirements for future weapon systems, the office updated acquisition and procurement policies to promote effective cybersecurity by adding an enclosure to its acquisition guidance, entitled *Cybersecurity in the Defense Acquisition System*. All three of these efforts demonstrate that DOD has taken actions toward implementing this one task.

However, while DOD has taken actions to implement this task, we found that the task had not been fully implemented. Officials from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics acknowledged that the task had not been fully implemented and that the office was on schedule for completing the initial 136 assessments by December 31, 2019, as required by statute. Similarly, DOD has made progress toward establishing cybersecurity requirements for future weapon systems, but the effort is not complete. In January 2017, the Joint Staff issued a memorandum that established a process requiring weapon systems to incorporate cyber resilience as they are designed and built. The process is undergoing a one-year trial period and is scheduled to be reassessed in 2018.

In addition, once tasks have been closed by the Principal Cyber Advisor, DOD has not continuously monitored task implementation; rather, monitoring occurs on a case-by-case basis. For example, officials from

²¹Pub. L. No. 114-92, § 1647 (2015).

the office of the Principal Cyber Advisor told us that the office approved the closure of a task to enhance the protection for critical acquisition programs and technology on the condition that the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics provide regular reports on progress in order to allow the Principal Cyber Advisor to track progress and provide assistance when necessary. Further, the officials from the office of the Principal Cyber Advisor told us that the office reserves the right to re-open or initiate reviews of closed tasks; as of April 2017, the office had not re-opened any closed tasks.

We have previously determined that DOD components do not consistently implement cybersecurity-related actions that are identified in DOD directives, instructions, or memorandums from senior DOD officials.²² In 2014, we reported on DOD's continuity planning and cyber resiliency efforts. DOD closed a related cyber resiliency task identified in *The DOD Cyber Strategy* after the department issued interim guidance for incorporating cyber resilience into DOD component continuity of operations plans; and DOD directed all of its components to establish or update their continuity of operations plans to include cyber resiliency measures by December 2017. While issuing a memorandum may have initiated the process, the task has not been fully implemented.

The Office of Management and Budget's *Management Responsibility for Enterprise Risk Management and Internal Control* provides guidance for management to identify risks and establish internal controls, as appropriate, to provide reasonable assurance that objectives are achieved and discusses the responsibility to continuously monitor the effectiveness of those internal controls.²³ *Standards for Internal Control in the Federal Government* explains that in defining objectives management should clearly define what is to be achieved, how it will be achieved, and the timeframes for achievement.²⁴ Further, the standards state that ongoing monitoring should be built into an entity's operations and be performed continually.

²²See GAO, *Defense Cybersecurity: DOD Needs to Better Plan for Continuity of Operations in a Degraded Cyber Environment and Provide Increased Oversight*, GAO-14-404SU (Washington, D.C.: Apr. 1, 2014). Also, see for example, DOD Inspector General, *DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued from August 1, 2015, through July 31, 2016*, DODIG-2017-034 (Dec. 13, 2016).

²³Office of Management and Budget, Circular A-123 (July 15, 2016).

²⁴[GAO-14-704G](#).

Based on these internal control standards, DOD's process is not sufficient to ensure the completion or implementation of tasks. Unless DOD modifies its process for deciding whether a task identified in *The DOD Cyber Strategy* is implemented, the department may not be able to ensure that the outcomes articulated in the strategy are achieved.

DOD Has Made Progress in Implementing the DOD Cybersecurity Campaign but Does Not Have Timeframes and Monitoring

DOD has made some progress in implementing the seven objectives required by the *DOD Cybersecurity Campaign*; however, the department does not have established timeframes for achieving full implementation. In June 2015, the DOD CIO; the Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Commander of CYBERCOM initiated a *DOD Cybersecurity Campaign* to identify specific actions that drive commanders and DOD senior leaders to enforce full cybersecurity compliance and accountability across the department. According to the *DOD Cybersecurity Campaign*, its goals are to educate commanders, civilian leaders, and all personnel responsible for the cybersecurity of the DOD information network on the risk to the mission. The three senior DOD leaders identified seven objectives to enable commanders and DOD senior leaders to enforce full cybersecurity compliance and accountability across the department. Table 7 below lists each of these objectives and shows our determination of the status of their implementation.

Table 7: Our Assessment of the Implementation Status of Department of Defense (DOD) Cybersecurity Campaign Objectives, as of March 2017

Objectives	Our Assessment of the Implementation Status
Develop a DOD Cybersecurity Scorecard to inform and achieve basic cybersecurity through the use of automated data collection in clearly defined areas.	In Progress
Execute the <i>DOD Cybersecurity Discipline Implementation Plan</i> that prioritizes the most critical hardening actions to counter adversary access to the DOD information network.	In Progress
Develop the framework for defensive cyberspace operations concept of operations that integrates defensive cyberspace operations and DOD information operations across the DOD information network forces, to include cyber protection teams and cybersecurity service providers.	Implemented
Execute priority initiatives for individual accountability, cybersecurity awareness, and education through the DOD Information Network Enterprise Cyber Readiness Executive Committee, with participation from the combatant commands.	In Progress
Establish a Platform Information Technology Working Group to focus on the cybersecurity of DOD platform information technology systems, including but not limited to weapon systems and industrial control systems.	Implemented

Objectives	Our Assessment of the Implementation Status
Upgrade the Command Cyber Readiness Inspection process to shift focus from a compliance inspection to a commander-driven operational risk assessment for cybersecurity readiness.	In Progress
Develop and implement a program to reinforce the traits and attributes of a healthy cybersecurity culture, modeled after other highly reliable organizations such as the nuclear enterprise, air traffic control, and weapons handling.	In Progress

Source: GAO analysis of DOD documentation. | GAO-17-512

As noted in the table above, DOD has implemented two of the objectives identified in the *DOD Cybersecurity Campaign*. Specifically, in February 2017, the DOD Information Security Risk Management Committee finalized a charter establishing a Platform Information Technology Cybersecurity Working Group to focus on the cybersecurity of DOD platform information technology systems, including but not limited to weapon systems and industrial control systems. According to the charter, this working group—chaired by the DOD CIO; the Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Commander of CYBERCOM—will provide expertise on the cybersecurity of platform information technology systems across DOD. A working group official explained that platform information technology is currently applicable to special purpose systems controlled and operated solely by technology, including industrial control systems.

The department has also implemented the *DOD Cybersecurity Campaign* objective to develop a framework for defensive cyberspace operations concept of operations that integrates defensive cyberspace operations and DOD information operations across the DOD information network forces. Specifically, in March 2017, the commander of CYBERCOM approved operational guidance titled, *Defensive Cyberspace Operations*. The operational guidance is applicable to CYBERCOM, all of its supporting elements, and all DOD components performing defensive cyberspace operations. Among other things, the guidance requires defensive cyberspace operations to be integrated with other cyberspace operations and information related activities. An official from CYBERCOM told us that the operational guidance came from the work to develop a concept of operations and was intended to address DOD’s need for guidance on defensive cyberspace operations.

DOD has also developed processes and procedures to monitor the implementation of four of the five *DOD Cybersecurity Campaign* objectives that are in the process of being implemented. Specifically, the DOD Cybersecurity Culture and Compliance Initiative monitors the department’s efforts in implementing two *DOD Cybersecurity Campaign*

objectives—(1) execute priority initiatives for individual cybersecurity awareness, and (2) develop and implement a program to reinforce the traits and attributes of a healthy cybersecurity culture. In addition, DOD uses the Cybersecurity Scorecard to monitor two other *DOD Cybersecurity Campaign* objectives that are in progress—development of a DOD Cybersecurity Scorecard and the execution of the *DOD Cybersecurity Discipline Implementation Plan*. According to DOD CIO officials, the Cybersecurity Scorecard has allowed for better oversight of DOD components' implementation of key cybersecurity measures and provides a forum for elevating issues to the Secretary of Defense. However, the scorecard is not fully implemented throughout the DOD components, and DOD continues to work on automating data collection to improve the data's reliability.²⁵ Additionally, recognizing the importance of resource prioritization, DOD CIO officials told us that the next phase is to move to a risk-based scorecard, which DOD expects to have implemented by March 2019.

While DOD has taken steps to implement the *DOD Cybersecurity Campaign* objectives that are still in process, the department does not know when it will achieve full implementation for one of the objectives because the department did not establish a timeframe for completing or monitoring it to help ensure accountability for full implementation. Specifically, the department does not have timeframes for the objective associated with transitioning to commander-driven operational risk assessments for cybersecurity readiness.

DOD has begun implementing the objective to shift the focus of its existing Command Cyber Readiness Inspection process to an operational cybersecurity readiness assessment. Specifically, the Defense Information Systems Agency and the Joint Force Headquarters-DOD Information Network are leading an effort to transition the department from a compliance-based Command Cyber Readiness Inspection process

²⁵As of February 2017, DOD acknowledged that there were data quality issues with all 11 assessed metrics monitored by the scorecard. Officials from the DOD components similarly informed us that they believe the scorecards do not reflect the most accurate information—a condition they attributed to limited automated data collection. The department has required the components to develop plans to automate data collection and provide reports that include budget, timelines, and other resources that will lead them to compliance by January 2018. These plans were originally supposed to be developed by November 30, 2015; however, as of April 2017, none of the DOD components had submitted these automation plans. Instead, CIO officials told us that the department was monitoring the DOD components' efforts to implement automation as part of the monthly scorecard.

to an operational risk-based inspection focused on missions, vulnerabilities, and threats—currently referred to as the Command Cyber Operational Readiness Inspection process—as the initial phase of CYBERCOM’s broader Command Cyber Readiness Inspection improvement initiative. According to the Joint Force Headquarters-DOD Information Network, the results of the new inspection process will be expressed in terms of risk to the mission and the department’s information network, unlike the previous readiness inspection process, which expressed results as pass or fail. DOD officials indicated that the new operational risk assessments will better allow DOD components to relate their cyber vulnerabilities to their mission. The department has piloted the new process in three organizations; however, DOD has not established a timeframe for implementation or identified a process to hold DOD leaders accountable for implementing these assessments across the department.

The Office of Management and Budget’s *Management Responsibility for Enterprise Risk Management and Internal Control* requires agencies to implement risk management in coordination with a number of internal control processes, including those contained in *Standards for Internal Control in the Federal Government*. *Standards for Internal Control in the Federal Government* highlight the need to (1) define objectives in specific terms, to include how objectives are to be achieved and timeframes for their achievement; and (2) enforce accountability by evaluating performance and holding organizations accountable.²⁶ Until the DOD CIO; the Under Secretary of Defense for Acquisition, Technology, and Logistics; and the Commander of CYBERCOM establish a timeframe for completing and a process for monitoring the objective associated with cybersecurity readiness assessments, DOD may be unable to assess its progress in achieving the objective, or to determine when it will achieve the strategic goals and objectives of the *DOD Cybersecurity Campaign*.

²⁶Office of Management and Budget Circular A-123 and [GAO-14-704G](#).

DOD Has Implemented Fifteen of Twenty-seven Cybersecurity Recommendations from Prior GAO Reports

As of March 2017, DOD had implemented 15 of the 27 cybersecurity recommendations (56 percent) we made in fiscal years 2011 through 2016. DOD is continuing to take actions to address 11 open recommendations, and 1 recommendation has been closed as not implemented. DOD’s 56 percent implementation rate is slightly lower than the government-wide 60 percent rate for implementing recommendations aimed at improving the security of federal systems and information.²⁷ Table 8 below shows our analysis of the implementation status of the 27 cybersecurity recommendations.

Table 8: Status of GAO Cybersecurity Recommendations by Report, Fiscal Years 2011 through 2016, as of January 2017

GAO Report	Recommendations			Open
	Total	Closed		
		Implemented	Not Implemented	
Fiscal Year 2011				
<i>Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities</i> (GAO-11-75)	4	4	0	0
<i>Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates</i> (GAO-11-695R)	2	2	0	0
Fiscal Year 2012				
<i>Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats</i> (GAO-12-762SU) ^a	8	7	1 ^b	0
Fiscal Year 2014				
<i>Defense Cybersecurity: DOD Needs to Better Plan for Continuity of Operations in a Degraded Cyber Environment and Provide Increased Oversight</i> (GAO-14-404SU) ^a	4	0	0	4
Fiscal Year 2015				
<i>Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems</i> (GAO-15-544)	4	0	0	4

²⁷In February 2017 we issued the 2017 High-Risk Series Update, which included “Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information.” We reported that federal agencies had implemented 1,500 of about 2,500—or 60 percent—recommendations aimed at improving the security of federal systems and information. GAO, *High-Risk Series, Progress on Many High-Risk Areas While Substantial Efforts Needed on Others*, [GAO-17-317](#) (Washington, D.C.: Feb. 15, 2017).

<i>Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning (GAO-15-749)</i>	1	1	0	0
<i>Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses (GAO-15-777)</i>	1	1	0	0
Fiscal Year 2016				
<i>Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents (GAO-16-332)^a</i>	1	0	0	1
<i>Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises (GAO-16-574)</i>	2	0	0	2
Fiscal Years 2011-2016 Grand Total	27	15	1	11

Source: GAO analysis of DOD data. | GAO-17-512

^aThese reports include recommendations that were identified in a letter we sent to the Secretary of Defense in August 2015 and September 2016 on DOD high-priority open recommendations.

^bThe recommendation from this report is not implemented and is no longer open. DOD updated several regulatory rules that officials believe address the problem. However, these rules do not prioritize efforts to protect information from companies or networks that are at the greatest risk based on an assessment of criticality, threat, and vulnerability, as the recommendation requires.

DOD Has Implemented More Than Half of Prior GAO Recommendations

As of March 2017, DOD had implemented 15 of the 27 cybersecurity recommendations (56 percent) we made in fiscal years 2011 through 2016. Among them are the following:

- Cyberspace Activities.** In July 2011, we reported on DOD's organization and planning of cyberspace operations, including its defensive and offensive efforts to address cybersecurity threats. DOD lacked clear and complete guidance on command and control responsibilities, and DOD did not have a comprehensive approach to assess its cyberspace capability needs and prioritize capability gaps.²⁸ We made 4 recommendations to strengthen DOD's cyberspace doctrine and operations to better address cybersecurity threats and ensure a more comprehensive approach to developing and prioritizing the department's cyberspace capability needs. DOD has implemented those 4 recommendations. In 2011, DOD updated its guidance related to cyberspace command and control relationships. In May 2012, DOD issued a capability gap assessment memorandum that includes DOD cyberspace capability gaps, proposed mitigation actions, and estimated completion dates. In February 2013, DOD issued a joint doctrine publication on cyberspace

²⁸GAO, *Defense Department Cyber Efforts: DOD Faces Challenges in Its Cyber Activities*, GAO-11-75 (Washington, D.C.: July 25, 2011).

operations. These actions allowed the department to take a more comprehensive approach to its cyberspace capabilities and clarify its cyberspace command and control relationships.

- **Cyberspace Budget Estimates.** In July 2011, we reported that DOD’s cybersecurity budget estimates did not include all full-spectrum cyberspace operations, including computer network attack, computer network exploitation, and classified funding costs. The department also lacked a central organization or a methodology for collecting and compiling budget information on cyberspace operations.²⁹ We made 2 recommendations to improve DOD’s ability to develop and provide consistent and complete budget estimates for its cyberspace operations. DOD implemented these recommendations by issuing new guidance for cyberspace operations budget submissions. The new guidance documents enabled DOD to develop a single cyberspace operations budget estimate that provides a complete picture of its cyberspace operations investments.
- **Small Business Cybersecurity Efforts.** In September 2015, we recommended that DOD identify and disseminate cybersecurity resources to defense small businesses, because DOD’s Office of Small Business Programs had not done so.³⁰ In their response to the draft report, DOD officials stated that the department would implement training events and education programs. Since then DOD has implemented this recommendation by making a reference guide for its workforce to use when engaging with small businesses. These steps better position defense small businesses to protect their information and networks from cyber threats.

DOD Has Not Yet Implemented Critical and High-Priority Cybersecurity Recommendations

DOD has not yet implemented 12 recommendations we have made to address cybersecurity weaknesses and strengthen its cyberspace posture. These 12 recommendations include 6 that address critical issues identified by *The DOD Cyber Strategy* and that we also previously identified as a priority for implementing. Among the recommendations not yet implemented (open, or closed as not-implemented) are the following:

²⁹GAO, *Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates*, [GAO-11-695R](#) (Washington, D.C.: July 29, 2011). The new budget guidance DOD developed is *Financial Management Regulation DOD 7000.14-R*, Volume 2B, Chapter 18, and Fiscal Year 2014 budget estimate guidance.

³⁰GAO, *Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses*, [GAO-15-777](#) (Washington, D.C.: Sept. 24, 2015).

-
- **Continuity of Operations.** In April 2014, we found that some DOD components had not developed continuity plans, conducted continuity exercises, or established oversight to hold the components accountable.³¹ Therefore, we made 4 recommendations to strengthen DOD’s cyber continuity program by: (1) updating DOD’s continuity guidance; (2) providing planning tools for exercises with cyber degradation; (3) increasing oversight of the components; and (4) evaluating its process for tasking the components and evaluating their continuity readiness. DOD concurred with and subsequently took actions to begin implementing the 4 recommendations; however, DOD has not fully implemented these recommendations. For example, DOD drafted an update to its defense continuity policy guidance, but as of January 2017, the revisions had not been completed. Without this guidance, it will be difficult for the DOD components to provide reasonable assurance that the systems and networks needed to maintain continuity of operations in a degraded cyber environment will be reliable, accessible, or available within needed timeframes.
 - **Insider Threat.** In June 2015, we made 4 recommendations to address challenges with DOD’s insider threat program—of which DOD concurred with two, and partially concurred with two.³² DOD is developing an insider threat implementation plan to address two of the recommendations, but that plan has not yet been published. DOD officials told us that the department is no longer taking action to address our recommendation to evaluate the extent to which its insider-threat programs address capability gaps. This recommendation originated in part when DOD did not complete a continuing analysis of gaps in security measures and of technology, policies, and processes that are needed to increase the capability of its insider-threat program to address these gaps, as required by statute.³³ This survey would have allowed DOD to define existing insider-threat program capabilities; identify gaps in security measures; and advocate for the technology, policies, and processes necessary to increase capabilities in the future. In their comments to the draft report, DOD officials stated that the department analyzes security gaps each quarter through its self-assessments, which identify program capability gaps. However, DOD has not evaluated and

³¹GAO-14-404SU.

³²GAO, *Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems*, [GAO-15-544](#) (Washington, D.C.: June 2, 2015).

³³Pub. L. No. 112-81, § 922 (2011).

documented the extent to which the current assessments describe existing insider-threat program capabilities, as required by law. Without a documented evaluation, the department will not know whether its capabilities to address insider threats are adequate, or whether the capabilities address statutory requirements.

- **Defense Civil Support.** In April 2016, we found that DOD’s guidance did not clearly define the roles and responsibilities of key DOD entities—such as DOD components—for domestic cyber incidents.³⁴ For example, U.S. Northern Command’s Defense Support of Civil Authorities response concept plan states that U.S. Northern Command would be the supported command for a mission to support civil authorities in responding to a domestic cyber incident. However, other guidance directs and DOD officials confirmed that a different command, CYBERCOM, would be responsible for supporting civil authorities in the event of a domestic cyber incident. Therefore, we made a recommendation that DOD issue or update guidance that clarifies roles and responsibilities to support civil authorities in a domestic cyber incident. DOD concurred with this recommendation. As of April 2017, the department had not implemented this recommendation, but officials indicated that they are in the process of drafting guidance that will clarify these roles. Specifically, the department is drafting a memorandum on defense support for cyber incident response that DOD officials believe will clearly articulate how DOD would support domestic cyber incident response efforts. DOD also scheduled exercises and a workshop to help it prepare to support civil authorities in the event of a cyber incident. However, until DOD clarifies the roles and responsibilities of its key entities for cyber incidents, it will remain unclear which DOD component or command should be providing support to civil authorities in the event of a major cyber incident.

We continue to believe that implementing these 12 recommendations would improve DOD’s cyberspace posture. We will continue to monitor DOD’s implementation of these recommendations, paying particular attention to the 6 high-priority recommendations that are still not implemented. Appendix I lists each report issued from fiscal years 2011 through 2016 that included recommendations for DOD, along with each recommendation’s implementation status.

³⁴GAO, *Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents*, [GAO-16-332](#) (Washington, D.C.: Apr. 4, 2016).

Conclusions

DOD continues to face complex and evolving cyberspace threats to its networks and information. It has taken actions to implement the tasks and objectives from the *DOD Cloud Computing Strategy*, *The DOD Cyber Strategy*, and the *DOD Cybersecurity Campaign*. However, gaps in the department's processes for monitoring implementation of this guidance limits DOD's ability to monitor the status of, and hold organizations accountable for, implementing key cybersecurity actions—such as its goal to identify, prioritize, and defend its most important networks and data so that it can carry out its missions effectively. DOD has made progress in implementing the seven actions required by the *DOD Cybersecurity Campaign*, but it does not know when it will achieve full implementation of one of the six remaining actions. DOD's continuing progress is highlighted by CYBERCOM's recent release of defensive cyber operations guidance in accordance with one of the objectives of the *DOD Cybersecurity Campaign*. Addressing the gaps in DOD's plans and timeframes for completing the remaining action will help DOD find and fix any root causes of cybersecurity breaches. Failure to implement this objective makes DOD vulnerable to cyber threats that may negatively affect mission readiness and could hinder mission accomplishment.

Recommendations for Executive Action

To ensure that DOD implements the tasks and objectives of key cybersecurity guidance to strengthen its cybersecurity posture, we recommend that the Secretary of Defense take the following two actions:

- Direct the Principal Cyber Advisor to modify the criteria for closing tasks from *The DOD Cyber Strategy* to reflect whether tasks have been implemented, and to re-evaluate tasks that have been previously determined to be completed to ensure that they meet the modified criteria;
- Direct the Commander of CYBERCOM, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics and DOD CIO, to establish a timeframe and monitor implementation of the *DOD Cybersecurity Campaign* objective to develop cybersecurity readiness assessments to help ensure accountability.

Agency Comments and Our Evaluation

We provided a draft of our report to DOD for review and comment. In its written comments, DOD partially concurred with both of our recommendations. DOD's written comments are reprinted in their entirety in appendix II. DOD also provided technical comments, which we incorporated into the report where appropriate.

DOD partially concurred with our recommendation to modify the criteria for closing tasks from *The DOD Cyber Strategy* to reflect whether tasks have been implemented and re-evaluate tasks that have previously been determined to be completed to ensure that they meet the modified criteria. The department stated that it has a robust process in place to ensure that tasks are normalized within appropriate processes, operations, and/or policies. DOD stated that it will implement internal control standards to periodically reassess closed tasks and that the department will re-evaluate the word “closed” as it relates to enduring activities that have active efforts ongoing across the department. If DOD implements these actions it will help ensure that the department monitors the status of these cybersecurity tasks to completion and will meet the intent of our recommendation.

DOD partially concurred with our recommendation to establish timeframes and monitor implementation of the *DOD Cybersecurity Campaign* objectives related to readiness assessments and a defensive cyberspace concept of operations to help ensure accountability. The department stated that CYBERCOM will coordinate with the necessary components to develop timelines for implementing these objectives. Further, the DOD CIO and the Under Secretary of Defense for Acquisition, Technology, and Logistics will monitor the status of these objectives to help ensure accountability. If DOD takes the actions it outlined, it will meet the intent of our recommendation. Because CYBERCOM provided us a copy of their recently published defensive cyber operations guidance before completion of our audit, we adjusted our recommendation to omit reference to a defensive cyberspace concept of operations.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Defense, DOD’s Deputy Principal Cyber Advisor, the Commander of CYBERCOM, the Acting Under Secretary of Defense for Acquisition, Technology, and Logistics, and DOD’s Acting Chief Information Officer. 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 me at (202) 512- 9971 or kirschbaumj@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

A handwritten signature in black ink that reads "Joe W. Kirschbaum" with a long horizontal stroke extending to the right from the end of the name.

Joseph W. Kirschbaum
Director
Defense Capabilities and Management

List of Committees

The Honorable John McCain
Chairman
The Honorable Jack Reed
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Richard Burr
Chairman
The Honorable Mark Warner
Vice Chairman
Select Committee on Intelligence
United States Senate

The Honorable Mac Thornberry
Chairman
The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Devin Nunes
Chairman
The Honorable Adam Schiff
Ranking Member
Permanent Select Committee on Intelligence
House of Representatives

Appendix I: Status of Cybersecurity Recommendations Made to the Department of Defense (DOD), Fiscal Years 2011 through 2016

Table 9 below summarizes the status of the 27 cybersecurity recommendations we made to DOD in 10 reports issued from fiscal years 2011 through 2016. We classify each recommendation as implemented, open, or not-implemented. Open and not-implemented recommendations are those that the agency has not yet taken sufficient steps to implement. Open recommendations are recommendations that the agency is still working toward implementing, while DOD is no longer taking actions on the recommendation that is not implemented. The recommendations are listed by report.

Table 9: GAO Cybersecurity and High-Priority Cyberspace Recommendations, Fiscal Years 2011 through 2016

GAO Recommendations	Status
Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities, GAO-11-75, July 25, 2011	
Develop a comprehensive capabilities-based assessment of the department-wide cyberspace-related mission and a timeframe for its completion.	Implemented
Clarify DOD guidance on command and control relationships between U.S. Strategic Command, the services, and the geographic combatant commands regarding cyberspace operations, and establish a timeframe for issuing the clarified guidance.	Implemented
Establish a timeframe for (1) deciding whether or not to proceed with a dedicated joint doctrine publication on cyberspace operations and (2) updating the existing body of joint doctrine to include complete cyberspace-related definitions.	Implemented
Develop an implementation plan and funding strategy for addressing any gaps resulting from the assessment that require new capability development or modifications to existing programs.	Implemented
Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates, GAO-11-695R, July 29, 2011	
Develop and document cyberspace-related definitions, including identifying specific activities and program elements, for purposes of budgeting for full-spectrum cyberspace operations that will be used and accepted department-wide. They should also establish a timeframe for completing these actions.	Implemented
Designate a single focal point to develop a methodology and provide a single, department-wide budget estimate and detailed spending data for full-spectrum cyberspace operations (to include computer network defense, attack, and exploitation), including unclassified funding as well as classified data from the military intelligence and national intelligence programs and any other programs, as appropriate.	Implemented
Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats, GAO-12-762SU, August 3, 2012	
Develop and issue an approved implementation plan for the program's expansion that (1) outlines its major tasks, (2) identifies and clarifies roles and responsibilities of stakeholders participating in the program, (3) defines metrics and timelines for measuring progress, (4) includes a comprehensive and realistic funding strategy to ensure that the program has the capability to absorb the projected increase in workload, and (5) describes a mechanism the program will use to periodically assess its expansion.	Implemented
Jointly develop a mechanism to enable participating defense industrial base companies to report cyber threat information to the government in order to improve the quality of indicators and signatures provided in the pilot, and identify the roles and responsibilities of stakeholders participating in the pilot and clarify who is responsible for providing additional information to participating defense industrial base companies about intrusions on their networks.	Implemented

**Appendix I: Status of Cybersecurity
Recommendations Made to the Department of
Defense (DOD), Fiscal Years 2011 through
2016**

Clearly link cybersecurity strategic goals with other risk management goals that are identified in updates to the Defense Industrial Base Sector-Specific Plan and the Joint Business Plan.	Implemented ^a
Identify a means to develop a list of defense industrial base networks to form a baseline for prioritization of cybersecurity efforts.	Implemented ^a
Facilitate the development, deployment, and awareness of voluntary risk and vulnerability self-assessments for cybersecurity threats.	Implemented ^a
Prioritize remediation or mitigation efforts for defense industrial base networks at greatest risk based on an assessment of criticality, threat, and vulnerability of DOD and non-DOD data on these networks.	Not Implemented ^{a,b}
Implement programs or take mitigation steps to protect critical DOD and non-DOD information that DOD and the Department of Homeland Security have identified as needing to be protected.	Implemented ^a
Accurately assess and report on the extent to which the defense industrial base sector is achieving cybersecurity goals and objectives in the Defense Industrial Base Sector Annual Report.	Implemented ^a
Defense Cybersecurity: DOD Needs to Better Plan for Continuity of Operations in a Degraded Cyber Environment and Provide Increased Oversight, GAO-14-404SU, April 1, 2014	
Revise DOD's continuity guidance to describe the priority of continuity planning, and provide additional guidance to the components on how to include accurate and complete data on information systems and networks necessary to perform mission-essential functions in their continuity plans. Such guidance should be consistent with Department of Homeland Security directives and, to the extent feasible, National Institute of Standards and Technology guidance.	Open ^a
Identify and provide DOD components tools that both emphasize the need for DOD components to conduct continuity exercises in a degraded cyber environment and assist components in developing and practicing effective responses during continuity exercises. The tools could include forums, multiyear frameworks for exercises to increase knowledge each year, exercise vignettes, and the use of the Raven Rock Mountain Complex's (also known as Site R) systems.	Open ^a
Refocus some of its resources to ensure that the office is fulfilling its Continuity Coordinator and oversight responsibilities. The oversight responsibilities should ensure that the components are meeting the department's continuity program policy and guidance, such as maintaining current continuity plans, exercising their continuity plans in a degraded cyber environment, and overseeing subcomponents' and subordinates' compliance with DOD's continuity policy and guidance.	Open ^a
Evaluate its approach to assigning tasks and evaluating the readiness of DOD components, including the potential use of existing mechanisms such as DOD tasking systems and the Defense Readiness Reporting System.	Open ^a
Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems, GAO-15-544, June 2, 2015	
Identify actions beyond the minimum standards that components should take to enhance their insider-threat programs in planned supplemental planning guidance to be developed.	Open
Evaluate and document the extent to which current assessments provide a continuing analysis of gaps for all DOD components; report to Congress on the results of this evaluation; and direct that the overall results of these self- and independent assessments be reviewed by the Office of the Under Secretary of Defense for Intelligence.	Open
Provide DOD components supplemental guidance that directs them to incorporate risk assessments into their insider-threat programs.	Open
Identify an insider-threat program office to support the Under Secretary of Defense for Intelligence's responsibilities in managing and overseeing DOD's and components' insider-threat programs.	Open
Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning, GAO-15-749, July 23, 2015	
Address challenges related to inventorying existing industrial control systems, identifying personnel with the appropriate expertise, and programming and identifying funding, as necessary.	Implemented

**Appendix I: Status of Cybersecurity
Recommendations Made to the Department of
Defense (DOD), Fiscal Years 2011 through
2016**

Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses, GAO-15-777, September 24, 2015

Identify and disseminate cybersecurity resources to defense small businesses as part of its existing outreach efforts.	Implemented
--	-------------

Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents, GAO-16-332, April 4, 2016

Issue or update guidance that clarifies roles and responsibilities for relevant entities and officials—including the DOD components, supported and supporting commands, and dual-status commander—to support civil authorities as needed in a cyber incident. ^c	Open ^a
--	-------------------

Defense Civil Support: DOD Needs to Identify National Guard’s Cyber Capabilities and Address Challenges in Its Exercises, GAO-16-574, September 6, 2016

Maintain a database that can fully and quickly identify the cyber capabilities that the National Guard in the 50 states, three territories, and the District of Columbia have and could use—if requested and approved—to support civil authorities in a cyber incident.	Open
---	------

Conduct a tier 1 exercise that will improve DOD’s planning efforts to support civil authorities in a cyber incident. Such an exercise should also address challenges from prior exercises, such as limited participant access to exercise environment, inclusion of other federal agencies and private-sector cybersecurity vendors, and incorporation of emergency or disaster scenarios concurrent to cyber incidents.	Open
--	------

Source: GAO analysis of DOD information. | GAO-17-512

^aThese recommendations were identified in letters we sent to the Secretary of Defense in August 2015 and September 2016 on high-priority areas.

^bThe recommendation from this report is not implemented and is no longer open. DOD updated several regulatory rules that DOD officials believe address the problem. However, these rules do not prioritize efforts to protect information from companies or networks that are at the greatest risk based on an assessment of criticality, threat, and vulnerability, as the recommendation requires.

^cIn a technical comment, DOD officials told us that they did not view this recommendation as a cybersecurity-related recommendation. However, we included this recommendation because DOD personnel can provide cybersecurity capabilities and services while coordinating, training, advising, and assisting cyber support and services provided that are incidental to military training to organizations and activities outside of DOD—including civil authorities in other departments and agencies of the U.S. government, state and local governments, non-governmental organizations, and the private sector. See Deputy Secretary of Defense Policy Memorandum 16-002, Cyber Support and Services Provided Incidental to Military Training and National Guard Use of DOD Information Networks, Software, and Hardware for State Cyberspace Activities (Washington, D.C.: May 24, 2016).

Appendix II: Comments from the Department of Defense



CHIEF INFORMATION OFFICER

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

JUN 28 2017

Mr. Joseph Kirschbaum,
Director, Defense Capabilities Management,
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 Government Accounting Office (GAO) Draft Report, GAO-17-512, 'DEFENSE CYBERSECURITY: DoD's Monitoring of Progress Implementing Cyber Strategies Can Be Strengthened,' dated May 26, 2017 (GAO Code 100920).

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense direct the Principal Cyber Advisor modify the criteria for closing tasks from the DoD Cyber Strategy to reflect whether tasks have been implemented and re-evaluate tasks that have been previously determined to be completed to ensure that they meet the modified criteria;

DoD RESPONSE: DoD partially concurs with the GAO recommendation.

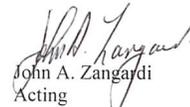
DoD has a robust process to ensure that Line of Effort objectives are codified or normalized with appropriate processes, operations, and/or policies in order to close the objective. DoD will implement internal control standards to periodically reassess "closed" Line of Effort tasks. DoD will also reevaluate the use of the word "closed" as it relates to enduring activities that have active efforts ongoing across the Department.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense direct DoD Chief Information Officer, in coordination with the Under Secretary of Defense for Acquisition, Technology and Logistics, and the Commander of USCYBERCOM establish a time frame for completing the objectives to develop cybersecurity readiness assessments and a defensive cyberspace concept of operations and monitoring to help ensure accountability for implementing these specific objectives of the *DoD Cybersecurity Campaign*.

DoD RESPONSE: DoD partially concurs with the GAO recommendation.

As an operational-level organization, USCYBERCOM will coordinate with necessary Components on developing a timeline for implementing specific objectives of the *DoD Cybersecurity Campaign* related to cybersecurity readiness assessments and a defensive cyberspace concept. The DoD Chief Information Officer, in coordination with USD(AT&L), will monitor and help ensure accountability.

Sincerely,


John A. Zangardi
Acting

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the individual named above, Tommy Baril, Assistant Director; Tracy Barnes; John Beauchamp; Lon Chin; Pamela Davidson; Ashley Houston; Jason Kelly; Amie Lesser; Randy Neice; and Cheryl Weissman made key contributions to this report.

Related Unclassified GAO Products

Defense Department Cyber Efforts: Definitions, Focal Point, and Methodology Needed for DOD to Develop Full-Spectrum Cyberspace Budget Estimates. [GAO-11-695R](#). Washington, D.C.: July 29, 2011.

Defense Department Cyber Efforts: DOD Faces Challenges In Its Cyber Activities. [GAO-11-75](#). Washington, D.C.: July 25, 2011.

Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities. [GAO-11-421](#). Washington, D.C.: May 20, 2011.

Defense Cyber Efforts: Management Improvements Needed to Enhance Programs Protecting the Defense Industrial Base from Cyber Threats. GAO 12-762SU, August 3, 2012.

Defense Cybersecurity: DOD Needs to Better Plan for Continuity of Operations in a Degraded Cyber Environment and Provide Increased Oversight. GAO-14-404SU, April 1, 2014.

Insider Threats: DOD Should Strengthen Management and Guidance to Protect Classified Information and Systems. [GAO-15-544](#), June 2, 2015.

Defense Infrastructure: Improvements in DOD Reporting and Cybersecurity Implementation Needed to Enhance Utility Resilience Planning. [GAO-15-749](#), July 23, 2015.

Defense Cybersecurity: Opportunities Exist for DOD to Share Cybersecurity Resources with Small Businesses. [GAO-15-777](#), September 24, 2015.

Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents. [GAO-16-332](#), April 4, 2016.

Defense Civil Support: DOD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises. [GAO-16-574](#), September 6, 2016.

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 GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

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, <http://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](#), [LinkedIn](#), [Twitter](#), and [YouTube](#). Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#). Visit GAO on the web at www.gao.gov and read [The Watchblog](#).

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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

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

