United States Government Accountability Office

Report to Congressional Committees

April 2020

CYBERSECURITY

DOD Needs to Take Decisive Actions to Improve Cyber Hygiene

Accessible Version

GAO-20-241

April 2020

CYBERSECURITY

DOD Needs to Take Decisive Actions to Improve Cyber Hygiene

GAO Highlights

Highlights of GAO-20-241, a report to congressional committees

Why GAO Did This Study

DOD has become increasingly reliant on information technology (IT) and risks have increased as cybersecurity threats evolve. Cybersecurity experts estimate that 90 percent of cyberattacks could be defeated by implementing basic cyber hygiene and sharing best practices, according to DOD's Principal Cyber Advisor.

Senate Report 115-262 includes a provision that GAO review DOD cyber hygiene. This report evaluates the extent to which 1) DOD has implemented key cyber hygiene initiatives and practices to protect DOD networks from key cyberattack techniques and 2) senior DOD leaders received information on the department's efforts to address these initiatives and cyber hygiene practices.

GAO reviewed documentation of DOD actions taken to implement three cyber hygiene initiatives and reviewed recurring reports provided to senior DOD leaders.

What GAO Recommends

GAO is making seven recommendations to DOD, including that cyber hygiene initiatives be fully implemented, entities are designated to monitor component completion of tasks and cyber hygiene practices, and senior DOD leaders receive information on cyber hygiene initiatives and practices. Of the seven recommendations, DOD concurred with one, partially concurred with four, and did not concur with two. GAO continues to believe that all recommendations are warranted.

View GAO-20-241. For more information, contact Joe Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov or Nick Marinos at (202) 512-9342 or marinosn@gao.gov.

What GAO Found

The Department of Defense (DOD) has not fully implemented three of its key initiatives and practices aimed at improving cyber hygiene. Carnegie-Mellon University defines cyber hygiene as a set of practices for managing the most common and pervasive cybersecurity risks. In discussions with GAO, DOD officials identified three department-wide cyber hygiene initiatives: the 2015 DOD Cybersecurity Culture and Compliance Initiative, the 2015 DOD Cyber Discipline Implementation Plan, and DOD's Cyber Awareness Challenge training.

- The Culture and Compliance Initiative set forth 11 overall tasks expected to be completed in fiscal year 2016. It includes cyber education and training, integration of cyber into operational exercises, and needed recommendations on changes to cyber capabilities and authorities. However, seven of these tasks have not been fully implemented.
- The Cyber Discipline plan has 17 tasks focused on removing preventable vulnerabilities from DOD's networks that could otherwise enable adversaries to compromise information and systems. Of these 17, the DOD Chief Information Officer is responsible for overseeing implementation of 10 tasks. While the Deputy Secretary set a goal of achieving 90 percent implementation of the 10 CIO tasks by the end of fiscal year 2018, four of the tasks have not been implemented. Further, the completion of the other seven tasks was unknown because no DOD entity has been designated to report on the progress.
- The Cyber Awareness training is intended to help the DOD workforce maintain awareness of known and emerging cyber threats, and reinforce best practices to keep information and systems secure. However, selected components in the department do not know the extent to which users of its systems have completed this required training. GAO's review of 16 selected components identified six without information on system users that had not completed the required training, and eight without information on users whose network access had been revoked for not completing training.

Beyond the initiatives above, DOD has (1) developed lists of the techniques that adversaries use most frequently and pose significant risk to the department, and (2) identified practices to protect DOD networks and systems against these techniques. However, the department does not know the extent to which these practices have been implemented. The absence of this knowledge is due in part to no DOD component monitoring implementation, according to DOD officials. Overall, until DOD completes its cyber hygiene initiatives and ensures that cyber practices are implemented, the department will face an enhanced risk of successful attack.

While two recurring reports have provided updates to senior DOD leaders on cyber information on the Cyber Discipline plan implementation, department leadership has not regularly received information on the other two initiatives and on the extent to which cyber hygiene practices are being implemented. Such information would better position leaders to be aware of the cyber risks facing DOD and make more effective decisions to manage such risks.

Contents

Tables

Figure

Abbreviations

CDIP	Cybersecurity Discipline Implementation Plan
DARPA	Defense Advanced Research Projects Agency
DC3I	DOD Cybersecurity Culture and Compliance Initiative
DISA	Defense Information Systems Agency
DOD	Department of Defense
DOD CIO	DOD Chief Information Officer
FISMA	Federal Information Security Modernization Act
IT	Information Technology
JFHQ	Joint Force Headquarters
DODIN	DOD Information Network

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 13, 2020

Congressional Committees

The Department of Defense (DOD) has become increasingly reliant on information technology (IT) systems and networks to conduct military operations and perform critical functions, such as logistics and budgeting. The security of these systems and data is vital to national security.

The risks to IT systems supporting DOD are increasing as cybersecurity threats continue to evolve and become more sophisticated. In particular, some foreign nations—where adversaries may possess sophisticated levels of expertise and significant resources to pursue their objectives—pose a significant threat. For example, according to the former Director of National Intelligence's 2019 *Worldwide Threat Assessment of the U.S. Intelligence Community*, China presents a growing attack threat to our core military systems and Russia is staging cyberattack assets to allow it to disrupt or damage U.S. military infrastructure.[1]

Compounding these threats, IT systems are often riddled with cybersecurity vulnerabilities—both known and unknown.[2] Cybersecurity vulnerabilities—particularly when combined with human error—can facilitate cyberattacks that disrupt critical operations, lead to inappropriate access to and modification of sensitive information, and threaten national security. Most of these cyberattacks can be attributed to human error—either through improperly configured IT systems or non-compliance with existing cybersecurity policy.[3] For example, the Defense Information

[1]*Worldwide Threat Assessment of the U.S. Intelligence Community, Hearing before the Senate Select Committee on Intelligence*, 116th Cong. (Jan. 29, 2019) (statement for the record, Daniel R. Coats, Director of National Intelligence).

[2]Department of Defense Inspector General, *Fiscal Year 2019 Top DOD Management Challenges* (Oct. 15, 2018).

[3]Department of Defense, Under Secretary of Defense for Acquisition, Technology and Logistics, DOD Chief Information Officer, and Commander, U.S. Cyber Command, *DOD Cybersecurity Campaign* (June 4, 2015) and Secretary of Defense and Chairman of the Joint Chiefs of Staff Memorandum, *Department of Defense Cybersecurity Culture and Compliance Initiative* (Sept. 30, 2015) which states that nearly all past successful network penetrations can be traced to one or more human errors that allowed the adversary to gain access to and, in some cases, exploit mission-critical information.

Systems Agency network was breached between May and July 2019 potentially compromising personal information, including Social Security numbers. Also, in July 2015, a phishing attack on the Joint Chiefs of Staff unclassified email servers resulted in the system being shut down for 11 days while cyber experts rebuilt the network, affecting the work of roughly 4,000 military and civilian personnel.[4] DOD has taken steps to address cybersecurity vulnerabilities, such as by establishing the Joint Force Headquarters DOD Information Network (JFHQ-DODIN) to serve as the DOD organization responsible for coordinating DOD defensive cybersecurity operations.

However, according to the department's Principal Cyber Advisor, cybersecurity experts estimate that about 90 percent of cyberattacks could be defeated by implementing basic "cyber hygiene and sharing best practices."[5] According to DOD officials, there is not a commonly-used definition for cyber hygiene in DOD doctrine, but Carnegie Mellon University's Software Engineering Institute defines cyber hygiene as a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.[6]

We discussed the definition of cyber hygiene with DOD officials to identify departmental initiatives aimed at improving cyber hygiene. DOD officials identified three departmental cyber hygiene initiatives: (1) the 2015 DOD Cybersecurity Culture and Compliance Initiative (DC3I), (2) the 2015 Cybersecurity Discipline Implementation Plan (CDIP), and (3) DOD's

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

[5]*Fiscal Year 2019 Review and Assessment of DOD Budget for Cyber Operations and U.S. Cyber Command: Hearing Before House Armed Services Comm., Emerging Threats and Capabilities Subcommittee*, 115th Cong. (Apr. 11, 2018) (statement of Kenneth P. Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor).

[6]Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices* (2017).

Cyber Awareness Challenge training.[7] In addition, we identified departmental practices to protect its networks from cyberattack techniques that adversaries may use. These practices include protective security controls and configurations.

Senate Report 115-262 accompanying a bill for the National Defense Authorization Act for Fiscal Year 2019 includes a provision that GAO assess policies governing DOD cyber hygiene and review threats to DOD from weaknesses in its cyber hygiene.[8] This report evaluates the extent to which (1) DOD has implemented key cyber hygiene initiatives and practices to protect DOD networks from key cyberattack techniques and (2) senior DOD leaders received complete information on the department's efforts to address the key cyber hygiene initiatives and key cyber hygiene practices.

To address our first objective, we reviewed the requirements in each of the three key cyber hygiene initiatives—the DC3I, CDIP, and DOD's Cyber Awareness Challenge. For the DC3I, we reviewed documentation from U.S. Cyber Command, the Office of the DOD Chief Information Officer (CIO), and the Joint Staff to identify and assess the specific actions these components had taken in response to the 11 tasks that were required by the Secretary of Defense and the Chairman of the Joint Chiefs of Staff.[9]

For the CDIP, we reviewed documentation and interviewed officials from the Office of the DOD CIO to identify and assess the extent to which the department had taken action to implement the 17 tasks that were required by the Deputy Secretary of Defense.[10] For the Cyber Awareness Challenge training, we obtained and analyzed information from the DOD CIO and a sample of 16 DOD components to determine the extent that

[7]Secretary of Defense and Chairman of the Joint Chiefs of Staff Memorandum, *Department of Defense Cybersecurity Culture and Compliance Initiative* (Sept. 30, 2015); Deputy Secretary of Defense Memorandum, *DOD Cybersecurity Campaign – Cybersecurity Discipline Implementation Plan* (Oct. 26, 2015); and DOD 8570.01-M, *Information Assurance Workforce Improvement Program* (Dec. 19, 2005, incorporating change 4, Nov. 10, 2015).

[8]See S. Rep. No. 115-262, at 358-359 (2018).

[9]DOD, Office of the Secretary of Defense Memorandum, *Department of Defense Cybersecurity Culture and Compliance Initiative* (Sept. 30, 2015).

[10]DOD, Deputy Secretary of Defense Memorandum, *DOD Cybersecurity Campaign - Cybersecurity Discipline Implementation Plan* (Oct. 26, 2015).

DOD personnel had taken the fiscal year 2018 Cyber Awareness Challenge training. These 16 components included the four military services, Joint Staff, three combatant commands, five defense agencies, two DOD field activities, and one component from the Office of the Secretary of Defense.[11] Further, we interviewed officials from Defense Information Systems Agency (DISA) and JFHQ-DODIN to determine the extent to which the department has implemented cyber hygiene practices to protect its networks from cyberattack techniques that adversaries may use.

To address our second objective, we defined senior leaders as the Secretary of Defense, the Deputy Secretary of Defense, and DOD component heads. In addition, we analyzed the contents of two recurring reports that senior leaders receive that describe efforts that the department is taking to improve the department's cybersecurity posture: the Cyber Hygiene Scorecard and the Cyber Landscape Report. In particular, we analyzed these reports to determine if they included information about DOD's implementation of key cyber hygiene initiatives that we discuss in the first objective. We describe our scope and methodology in more detail in appendix I.

We conducted this performance audit from January 2019 to April 2020 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.

[11]We accounted for the size of the non-service and non-combatant command components in our sample by including the larger defense agencies and the smaller DOD field activities. We chose the ratio of five defense agencies and two DOD field activities to reflect the ratio of agencies to field activities in DOD. That is, defense agencies are about 71 percent of DOD's non-service and non-combatant command components and about 71 percent of our sample. We selected the following components in our sample: U.S. Air Force, U.S. Army, U.S. Marine Corps, U.S. Navy, the Joint Staff, U.S. European Command, U.S. Strategic Command, U.S. Southern Command, the Defense Advanced Research Projects Agency, the Defense Commissary Agency, the Defense Contract Management Agency, the Defense Finance and Accounting Service, the National Security Agency, the Defense Media Activity, the Defense Technology Security Administration, and the Office of the DOD Chief Information Officer.

Background

Key DOD Cyber Hygiene Initiatives

DOD officials identified three key department-wide initiatives that include a number of cybersecurity practices aimed at improving cyber hygiene: the DC3I, the CDIP, and the Cyber Awareness Challenge training. These efforts recognize the importance of command leadership, best practices for DOD network users, and technical countermeasures against cybersecurity threats.

- **DC3I.** In September 2015, the Secretary of Defense and the Chairman of the Joint Chiefs of Staff signed the DC3I in an effort to transform DOD cybersecurity culture by enabling and reshaping leaders, cyber providers, personnel who perform cyberspace operations, and general users to improve individual human performance and accountability on DOD's network. The DC3I memorandum identifies 11 tasks assigned to various DOD components to respond to and implement across the department—such as the development of cybersecurity training briefs for DOD leadership, integration of cybersecurity into operational training and exercises, and the development of a resourcing plan to support scheduled inspections of units conducting cyberspace operations. From September 2015 to December 2016, U.S. Cyber Command was initially responsible for ensuring that relevant components implemented the DC3I. In December 2016, the Deputy Secretary of Defense assigned the DOD CIO as the official responsible for ensuring that components implemented the initiative because, in part, the DOD CIO has DOD-wide oversight authority.
- **CDIP.** The CDIP is one of seven actions identified in DOD's *Cybersecurity Campaign* to prompt commanders and senior leaders to enforce full cybersecurity compliance and accountability across the department. In October 2015, the Deputy Secretary of Defense signed the CDIP to reinforce basic cybersecurity technical requirements identified in policies, directives, and orders as a means to defend DOD information networks, secure DOD data, and mitigate risks to DOD missions. The CDIP memorandum identifies 17 tasks for all commanders and supervisors to implement across the department. These tasks include removing operating system software that no longer receives security updates from vendors, configuring servers consistent with DOD guidance on secure configurations, and

addressing vulnerabilities for servers and network infrastructure in a timely manner.

- **Cyber Awareness Challenge Training.** This training is intended to help the DOD workforce (including service members, civilians, and contractors) to maintain awareness of known and emerging cybersecurity threats, reinforce best practices to keep information and information systems secure, and ensure that network users stay abreast of changes in DOD cybersecurity policies. DISA develops the training content and periodically updates the training. In addition, the Cyber Workforce Advisory Group that includes officials from the DOD CIO, DISA, and DOD components, solicit input about ways to improve the training and meets annually to approve updates to the Cyber Awareness Challenge.

Increasing Cybersecurity Awareness and Accountability at Leadership Levels

Federal law and a DOD initiative and strategy highlight the important role of leadership in improving cybersecurity culture and performance across the department. For example, the Federal Information Security Modernization Act of 2014 (FISMA) requires agency heads—including the Secretary of Defense—to ensure that senior agency officials provide security for the information and information systems that support the operations and assets under their control.[12] Additionally, the DC3I states that leaders will be held accountable by the chain of command for the cybersecurity performance of their organization and the individuals who comprise it, and for the role cybersecurity performance plays in accomplishing assigned missions. It also states that leaders will set an example and help individuals master appropriate cyber behavior, will take action against those who commit gross negligence or errors of commission, and may use all available means, both legal and administrative, as they deem appropriate.

Further, the 2018 DOD Cyber Strategy states that reducing the department's network attack surface (i.e., the different points in a network where attackers can try to enter or extract information) requires an increase in cybersecurity awareness and accountability across the department. The strategy also states that the department would hold DOD personnel accountable for their cybersecurity practices and choices.

[12]Pub. L. No. 113-283 (2014) and codified as amended at 44 U.S.C. § 3554(a)(2).

The 2019 *Cybersecurity Readiness Review,* directed by the Secretary of the Navy, describes best practices for effective cybersecurity leadership.[13] These best practices, according to the readiness review, require Navy leaders to be informed on cybersecurity issues facing their organization, engaged in ensuring cybersecurity issues are addressed, and hold their organization accountable for cybersecurity performance.

Key Cybersecurity Roles and Responsibilities

A number of DOD officials and components have key roles and responsibilities for cybersecurity, including the three key cyber hygiene initiatives. For example:

- **Secretary and Deputy Secretary of Defense.** FISMA makes the Secretary of Defense responsible for providing information security protections commensurate with the risk and magnitude of harm facing the department.[14] In addition, Executive Order 13800, issued in May 2017, aligns with FISMA by holding agency heads accountable for implementing risk management measures commensurate with the risk and magnitude of the harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of IT and data.[15]
- **DOD Chief Information Officer.** FISMA requires DOD to develop, document, and implement a program to provide security for information and information systems (commonly referred to as a cybersecurity program) and directs the Secretary of Defense to delegate to the DOD CIO (and military department CIOs) authority to ensure compliance with the law.[16] In addition, the DOD CIO is responsible for overseeing implementation of the three key cyber hygiene initiatives.

[13]*Secretary of the Navy Cybersecurity Readiness Review*, (Mar. 4, 2019) is a review of the Department of the Navy's cybersecurity posture directed by the Secretary of the Navy following the loss of a significant amount of sensitive Navy data.

[14]44 U.S.C. § 3554 (a)(1). By delegation, the Deputy Secretary of Defense has full power and authority to act for the Secretary of Defense and to exercise the powers of the Secretary of Defense on all matters for which the secretary is authorized to act pursuant to law.

[15]Exec. Order No. 13,800 *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22,391 (May 16, 2017).

[16]44 U.S.C. § 3554(b) and § 3554 (a)(3).

- **DOD Component heads.** DOD component heads are responsible for ensuring that IT under their purview complies with DOD Instruction 8500.01.[17] In addition, component heads are responsible for ensuring that their network users complete annual security awareness training.
- **DOD Component CIOs.** DOD component CIOs are responsible for developing, implementing, maintaining, and enforcing a component cybersecurity program on behalf of their respective component heads.[18] In doing so, component CIOs are responsible for ensuring that their components implement the CDIP tasks.
- **Chairman of the Joint Chiefs of Staff.** The Chairman of the Joint Chiefs of Staff is responsible for advising the President and Secretary of Defense on operational policies, responsibilities, and programs. The Chairman also assists the Secretary of Defense in implementing operational responses to cyber threats and ensures cyberspace plans and operations are compatible with other military plans and operations.[19] The staff members who support the Chairman of the Joint Chiefs of Staff are referred to as the Joint Staff, which is comprised of members from all of the military services.
- **U.S. Cyber Command.** The Commander of U.S. Cyber Command has the mission to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. In addition, the Commander is responsible for, among other things, issuing orders and directives to all DOD components for the execution of global operations aimed at securing and defending the department's networks.[20]
- **Defense Information Systems Agency.** The Director of DISA is responsible for developing, implementing, and managing cybersecurity for the department's network and works with other components to secure DOD systems. For example, the Director is

[17]Department of Defense Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014, incorporating Change 1, Oct. 7, 2019).

[18]Department of Defense Instruction 8500.01, *Cybersecurity* (Mar. 14, 2014, incorporating Change 1, Oct. 7, 2019).

[19]Chairman of the Joint Chiefs of Staff, Joint Publication 3-12, *Cyberspace Operations* (June 8, 2018).

[20]This responsibility is delegable to the commander of JFHQ-DODIN.

responsible for developing cybersecurity awareness training for all users on DOD's network.

- **JFHQ-DODIN.** The Commander of JFHQ-DODIN is responsible for, among other things, commanding, controlling, planning, directing, coordinating, integrating, and synchronizing DOD defensive cybersecurity operations.[21] JFHQ-DODIN also performs two types of cyber readiness inspections to ensure DOD units comply with requirements related to network security and to evaluate the ability of units to accurately detect and mitigate vulnerabilities and anomalous activity on DOD's network.[22]

Cybersecurity Is a High-Risk Area

The security of federal cyber assets has been on our High-Risk List since 1997. In September 2018, we issued an update to this high-risk area that identified actions needed to address cybersecurity challenges facing the nation—including improving implementation of government-wide cybersecurity initiatives aimed at securing federal systems and information.[23] We also have identified ensuring the cybersecurity of the nation as one of nine high-risk areas that need especially focused executive and congressional attention.[24]

In August 2017, we reported on DOD's progress in implementing the department's cyber strategies. We found that DOD had implemented the cybersecurity elements of the DOD Cloud Computing Strategy and had made progress in implementing the 2015 DOD Cyber Strategy and DOD Cybersecurity Campaign, which was comprised of multiple initiatives

[21]Department of Defense Instruction 8010.01, *Department of Defense Information Network (DODIN) Transport*, (Sept. 10, 2018). The Director of the Defense Information Systems Agency, under the authority and direction of the CIO, also serves as the commander of JFHQ-DODIN.

[22]The Command Cyber Readiness Inspections evaluate an organization's compliance with DOD security orders and directives, and with assessing network vulnerabilities, physical and traditional security, and user education and awareness. The Command Cyber Operational Readiness Inspections provide combatant commands and federal agencies with a greater understanding of the operational risk their missions face because of their cybersecurity posture (assessing mission, threat, and vulnerabilities).

[23]GAO, *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[24]GAO, High-Risk Series: *Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: Mar. 6, 2019).

including the CDIP.[25] However, DOD's process for monitoring implementation of the DOD Cyber Strategy resulted in the closure of tasks before they were fully implemented. We also found that DOD lacked a timeframe and process for monitoring implementation of the DOD Cybersecurity Campaign objective to transition to commander-driven operational risk assessments for cybersecurity readiness. We recommended that DOD (1) modify criteria for closing tasks as implemented and reevaluate tasks previously determined to be completed to ensure they meet modified criteria and (2) establish a timeframe and monitor implementation of the DOD *Cybersecurity Campaign* objective to develop cybersecurity readiness assessments to help ensure accountability. DOD partially concurred with both recommendations. As of January 2020, neither recommendation had been implemented.

DOD Has Not Fully Implemented Key Cyber Hygiene Initiatives and Does Not Know the Extent of Protection

DOD has not fully implemented its three cyber hygiene initiatives. Specifically, (1) the DOD CIO and DOD components have not implemented seven of the 11 DC3I tasks due in fiscal year 2016; (2) DOD has implemented six of 10 CDIP tasks that the DOD CIO oversees and does not know the extent that seven other CDIP tasks are implemented; and (3) DOD did not know the extent to which users for selected components completed the Cyber Awareness Challenge training in 2018 and one component did not use the required training. In addition, the department does not know the extent that cyber hygiene practices to protect its networks from key cyberattack techniques have been implemented.

DOD Has Not Implemented Seven of the 11 DC3I Tasks Due in Fiscal Year 2016

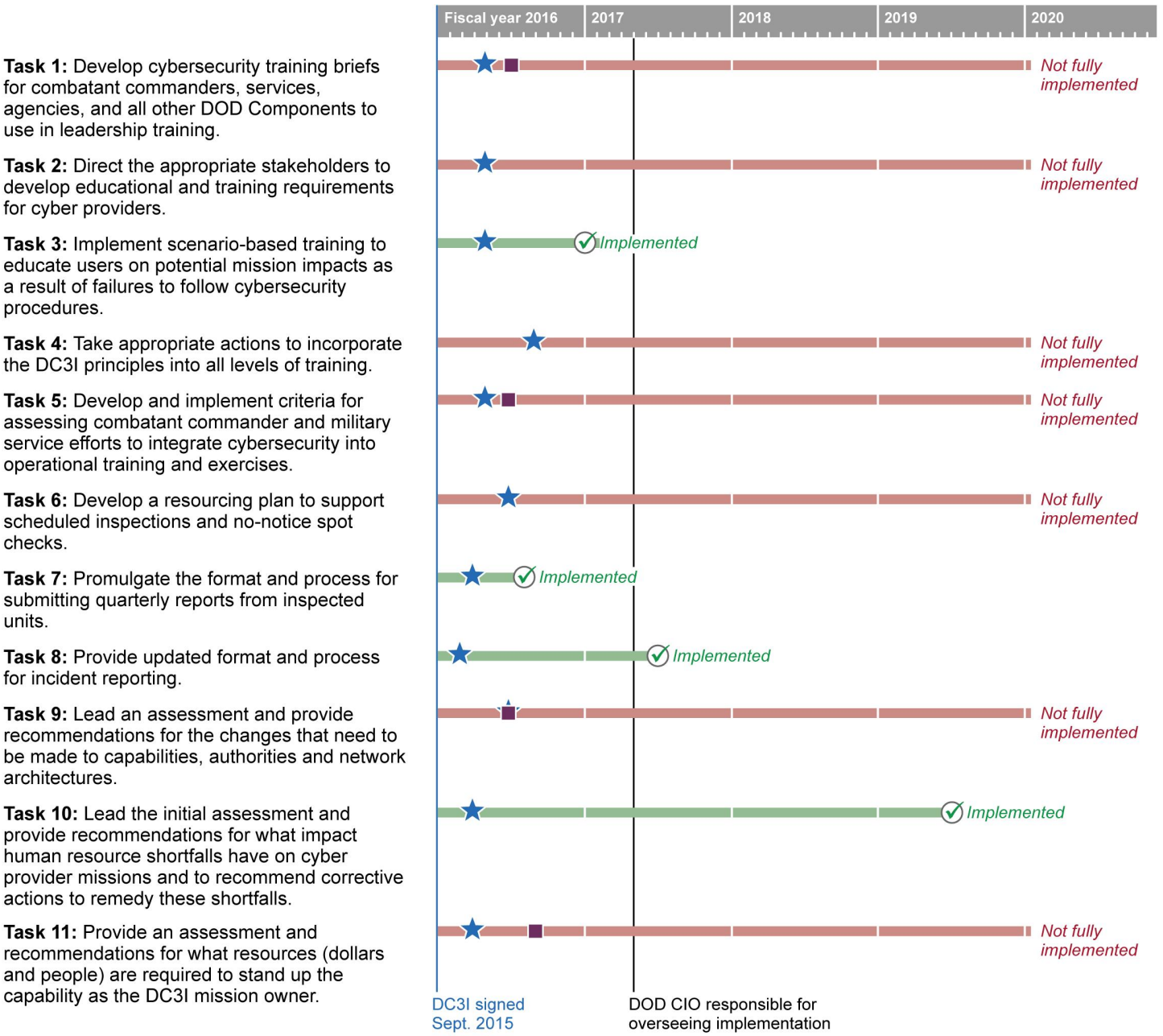
DOD has not implemented seven of the 11 DC3I tasks despite fiscal year 2016 deadlines for each of the tasks being established by the

[25]GAO, *DOD Cybersecurity: DOD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened*, GAO-17-512, (Washington, D.C.: Aug. 1, 2017).

department.[26] In particular, DOD components have implemented four DC3I tasks and have not implemented the seven remaining tasks, as shown in figure 1.

[26]Secretary of Defense and Chairman of the Joint Chiefs of Staff Memorandum, *Department of Defense Cybersecurity Culture and Compliance Initiative* (Sept. 30, 2015). Specifically, the Secretary of Defense and Chairman of the Joint Chiefs of Staff tasked specific DOD components to take actions to implement the 11 DC3I tasks within 60, 90, 120, or 180 days. The memorandum assigned responsibilities for specific tasks to U.S. Cyber Command, the Office of the DOD CIO, Joint Staff, combatant commanders, service chiefs, and agency and DOD component heads.

Figure 1: Implementation Status of DOD Cybersecurity Culture and Compliance Initiative (DC3I) Tasks



Source: GAO analysis of Department of Defense (DOD) information. | GAO-20-241

Note: DOD officials told us that the department continues to take action to implement tasks 2 and 6. DOD CIO officials estimate that DOD will implement the cyber provider training task in April 2020. U.S. Cyber Command officials told us the department is developing a resourcing plan, but the command did not provide an estimate as to when it would implement the task. Appendix II provides additional details on the implementation of each task.

As shown above, DOD has implemented four DC3I tasks.[27] For example, DOD CIO implemented a task that requires that office to assess the effect of cyber workforce shortfalls on DOD's mission and provide recommendations to address these shortfalls (task 10 in figure 1 above). Specifically, in April 2019, DOD CIO provided a plan to the Office of Personnel Management to address cyber workforce shortages by filling vacant positions, enhancing outreach and recruitment, and expanding on hiring authorities.[28]

However, DOD has not implemented the remaining seven DC3I tasks. For example:

- **DOD has not fully implemented leadership cybersecurity training briefs (task 1).** In April 2016, U.S. Cyber Command developed two training briefs to be used in leadership training. However, as of October 2019, DOD components have not received either training brief, according to DOD officials. In September 2016, U.S. Cyber Command provided the Deputy Secretary of Defense a DC3I status report and informed him that two products were developed to address this task and that they would be disseminated to DOD components.[29] However, as of October 2019, neither U.S. Cyber Command nor the Office of the DOD CIO had disseminated these leadership training

[27]We determined that a DC3I task was implemented when the assigned DOD components completed all of the objectives of a task, as appropriate.

[28]In a March 2019 review of cybersecurity workforce management, we recommended that DOD complete the identification and coding of vacant positions in the department performing IT, cybersecurity, or cyber-related functions. DOD concurred with this recommendation, and stated that its longer-term initiative is to code positions, including vacant positions, in DOD's manpower requirements system to provide true gap analysis capabilities. See GAO, *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C.: Mar. 12, 2019).

[29]In December 2016 (i.e., three months after the status report), the Deputy Secretary of Defense issued a memorandum to the DOD CIO and commander of U.S. Cyber Command approving the transition of DC3I mission lead from U.S. Cyber Command to the DOD CIO in alignment with DOD Directive 5144.02, *DOD Chief Information Officer (DOD CIO)*. The DOD CIO was supposed to leverage existing authorities and departmental efforts to lead and provide oversight of cybersecurity culture and compliance transformation.

briefs across the department, according to DOD officials.[30] In reviewing the training briefs, we found that, if they had been incorporated into DOD leadership training, leaders would have been better positioned to address cybersecurity risks. For example, they may have learned, among other things, how to understand, assess, and interpret cyber-reportable events and incidents and how they affect military operations.

- **DOD has not developed cyber-provider training (task 2).** In February 2019, the office of the DOD CIO completed a review of all military and civilian IT positions to identify the work roles of all cyber providers in the department. However, the office has not developed educational and training requirements for cyber providers. DOD CIO officials told us that, consistent with task 2, they are drafting a DOD Manual, *Cyber Workforce Qualification and Management Program*, which would document educational and training requirements for the work roles for each cyber provider. DOD CIO officials expect to complete the manual around April 2020.
- **DOD has not fully implemented criteria for assessing cybersecurity in operational training and exercises (task 5).** In March 2016, the Joint Staff developed criteria for assessing military service and combatant command efforts to integrate cybersecurity into operational training and exercises. For example, the Joint Staff developed a checklist of cybersecurity elements that should be included in cyberspace-related training objectives and assessed during training events. In May 2016, the Vice Chairman of the Joint Chiefs of Staff required that the criteria be used to assess military service and combatant command efforts to integrate cybersecurity into operational training and exercises. In May 2019, Joint Chiefs of Staff officials told us the criteria was not incorporated into the Chairman's annual training guidance, citing personnel turnover, and that they do not have plans to incorporate the criteria. According to the DC3I, operational and tactical commanders and leaders need to interpret the effect that cyber insecurity may have on the mission and integrate cyber effects into mission planning. If Joint Staff had updated the Chairman of the Joint Chiefs of Staff guidance for operational training, DOD commanders would have had criteria they

[30]DOD CIO officials told us that they did not have a record that the office had received copies of these training briefs; however, U.S. Cyber Command officials told us that the command had provided copies of the training briefs to the office. Regardless of whether the training briefs were provided at the time, the September 2016 status report (which both DOD components had received) stated that training briefs had been developed and were ready to be transmitted to DOD components.

could use to assess the effect that cyber insecurity may have on military missions.

The lack of progress in implementing the tasks occurred, in part, because the DOD CIO did not take steps to ensure that the DC3I tasks were implemented. DOD CIO officials told us they were not aware of their responsibility to oversee implementation of the DC3I. Initially, U.S. Cyber Command was assigned as the entity responsible for overseeing implementation of the DC3I; however, in December 2016, the Deputy Secretary of Defense approved the transition of the DC3I mission lead to the department's CIO.[31] According to this transition memorandum, the CIO was to leverage existing authorities and departmental efforts to lead and provide oversight of cybersecurity culture and compliance transformation. Additionally, DOD CIO officials told us that the office is focusing its resources on other CIO initiatives, such as implementing the cyber landscape initiative.[32] However, the DC3I included a task (task 11 in figure 1 above) that required an assessment of the resources needed to ensure that DOD implemented the DC3I and this task had not been completed at the time of our review. If DOD CIO does not take appropriate steps to ensure that the DC3I tasks are implemented, the department risks compromising the confidentiality, integrity, and availability of mission-critical information as a result of human error by users on the department's networks.

[31]Deputy Secretary of Defense Memorandum, *Transfer of Mission Lead for Department of Defense Cybersecurity Culture and Compliance Initiative* (Dec. 19, 2016).

[32]According to the DOD CIO, the cyber landscape initiative prioritizes where and how DOD should apply resources and innovations to execute DOD's 2018 Cyber Strategy. The cyber landscape focuses on remediation strategies for a complex cyber landscape, whose components range from information and networks to DOD's cyber workforce and supply chain risk management.

DOD Has Implemented Six of 10 CDIP Tasks That the DOD CIO Oversees and Does Not Know the Extent That Seven Other CDIP Tasks Have Been Implemented

DOD Has Implemented Six of 10 CDIP Tasks That the DOD CIO Oversees

Since 2015, DOD has implemented six of 10 CDIP tasks that the DOD CIO is to oversee, but has not achieved desired performance targets for the remaining four tasks even though there is a requirement to implement all 10 by the end of fiscal year 2018.[33] In the 2015 CDIP memorandum, the Deputy Secretary of Defense directed DOD components to implement all 17 CDIP tasks for all system users, IT hardware, and IT software to remove preventable vulnerabilities from DOD's network that could allow adversaries to compromise information and information systems. According to a March 2019 memorandum, the Deputy Secretary of Defense challenged the department to achieve 90 percent implementation of the 10 CDIP tasks overseen by DOD CIO by the end of fiscal year 2018. In table 1, we list the 17 tasks and indicate the 10 tasks that the department's CIO oversees.

[33]The CDIP memorandum requires the Office of the DOD CIO to report on the progress that components have made in implementing 10 of the CDIP tasks.

Table 1: Cyber Discipline Implementation Plan (CDIP) Tasks Overseen by the DOD Chief Information Officer (CIO) and Tasks That Are Not Overseen

CDIP tasks	Overseen by DOD CIO	Not Overseen
1: Commanders and supervisors must ensure 100 percent use of separate public key infrastructure (PKI)-based authentication credentials for system administrators on any DOD Information Network (DODIN) and disable username/passwords.[a]	Overseen by DOD CIO	
2: Commanders and supervisors will review all Internet-facing assets to ensure they are hosted in a DOD demilitarized zone (DMZ) and disconnect all Internet-facing web servers and web applications without an operational requirement.[b]	Overseen by DOD CIO	
3: Commanders and supervisors will ensure no Internal DODIN active directory trusts any DOD DMZ or external active directory.[c]		Not Overseen by DOD CIO
4: Commanders and supervisors must ensure their web servers and web applications internal to unclassified networks (not in a DOD DMZ) require DOD-approved PKI user authentication.	Overseen by DOD CIO	
5: Commanders and supervisors must ensure their web servers and web applications hosting controlled unclassified information within a DOD DMZ require DOD-approved PKI user authentication.	Overseen by DOD CIO	
6: Commanders and supervisors must ensure their web servers and web applications residing on Secret-level networks require DOD-approved PKI user authentication.	Overseen by DOD CIO	
7: Commanders and supervisors will ensure any login to a network infrastructure device requires PKI-based authentication/credentials.	Overseen by DOD CIO	
8: Commanders and supervisors will ensure the upgrade or removal of Windows XP and Windows Server 2003 operating systems on the DODIN.	Overseen by DOD CIO	
9: Commanders and supervisors will ensure endpoint security solution is in compliance with the Operation Cyber Shield order.[d]	Overseen by DOD CIO	
10: Commanders and supervisors must ensure all servers and network infrastructure devices are compliant with all current patch releases.[e]	Overseen by DOD CIO	
11: Commanders and supervisors will ensure secure configuration of all physical and virtual servers in accordance with DOD security standards.[f]	Overseen by DOD CIO	
12: Commanders and supervisors will ensure hyperlinks are disabled in Outlook email clients on unclassified and classified networks.		Not Overseen by DOD CIO
13: Commanders and supervisors will ensure hyperlinks are disabled for mobile devices.		Not Overseen by DOD CIO
14: Commanders and supervisors will ensure physical security of their network infrastructure devices.		Not Overseen by DOD CIO
15: Commanders and supervisors will report all commercially provided internet connections to DOD's unclassified network.		Not Overseen by DOD CIO
16: Commanders and supervisors will ensure alignment to a Computer Network Defense Service Provider (CNDSP).		Not Overseen by DOD CIO
17: Commanders and supervisors with CNDSP responsibility will ensure the cyber incident response plan(s) are properly exercised and documented.		Not Overseen by DOD CIO

Source: GAO analysis of Department of Defense (DOD) information. | GAO-20-241

[a]Public Key Infrastructure, or PKI, is a system of hardware, software, policies, and people that, when fully and properly implemented, can provide a suite of information security assurances that are important in protecting sensitive communications and transactions.

[b]The "demilitarized zone," commonly referred to as the DMZ, is the perimeter network segment that exists between the perimeter firewall connected to the internet and the organization's private network.

[c]Microsoft Active Directory is used, among other things, to authenticate users and verify access systems and information. Active Directory trusts enable organizations to grant access to users in other Active Directory environments. Active Directory environments that are external to DOD's internal networks are at increased risk of compromise. If internal Active Directory environments trust external environments, increased risk exists that malicious actors could exploit that trust and compromise the confidentiality, integrity, and availability of systems associated with the internal Active Directory environments.

[d]Endpoint security solutions are safeguards implemented through software to protect end-user machines (e.g., workstations and laptops) against attack. These safeguards can include antivirus, antispyware, anti-adware, personal firewalls, and host-based intrusion detection and prevention systems.

[e]Patches correct security and functionality problems in software and firmware.

[f]Secure configurations are designed to reduce the organizational security risk from operation of a system, and may involve using trusted or approved software loads, maintaining up-to-date patch levels, applying secure configuration settings of the IT products used, and implementation of endpoint protection platforms. Secure configurations for a system are most often achieved through the application of secure configuration settings to the IT products (e.g., operating systems, databases, etc.) used to build the system.

The department has achieved its performance targets for six of the 10 CDIP tasks that the DOD CIO oversees. For example, in October 2018 DOD achieved its performance target for one task that requires the department to move all of DOD's web servers into a DOD "demilitarized zone," or DMZ, according to DOD's fiscal year 2018 Federal Information Security Modernization Act report to the director of the Office of Management and Budget.[34] Placing these web servers in a DMZ directs web traffic intended for those servers—including malicious traffic—to systems within perimeter firewalls that screen the traffic before allowing access to organizations networks.[35] By implementing the task and moving 11,000 web servers into the DMZ, DOD has reduced the risk that malicious traffic can reach its web servers.

However, the department has not achieved the department-wide goal for the four remaining CDIP tasks overseen by DOD CIO.[36] For example,

[34]The "demilitarized zone," commonly referred to as the DMZ, is a perimeter network segment that exists between the perimeter firewall connected to the internet and the organization's private network.

[35]According to the National Institute of Standards and Technology (NIST), a firewall is an inter-network gateway that restricts data communication traffic to and from one of the connected networks (the one said to be "inside" the firewall) and thus protects that network's system resources against threats from the other network (the one that is said to be "outside" the firewall).

[36]Specific information about the tasks that were not fully implemented and the implementation rate for the individual DOD components is classified and will be included in a classified version of the report.

DOD did not achieve its performance target for a task that required components to ensure they were compliant with endpoint security guidance.[37] DOD CIO officials told us that the remaining four CDIP tasks are challenging for the department to achieve the 90 percent performance target because some DOD components use aging information technology systems and these older systems may not be equipped to implement all CDIP tasks. We have previously reported that legacy systems have operated with known cybersecurity vulnerabilities that are either technically difficult or prohibitively expensive to address.[38] In light of the security risks posed by DOD component legacy systems, we stated that it is imperative that agencies carefully plan for their successful modernization.

DOD did not achieve the 90 percent goal for four of the 10 CDIP tasks by the end of fiscal year 2018 due in part to DOD components not developing plans with scheduled completion dates to implement these four tasks, according to DOD officials. DOD CIO officials told us that they had not required DOD components to develop plans with scheduled completion dates for the remaining four CDIP tasks. CIO officials believed that the DOD components would implement the CDIP memorandum since it was signed by the Deputy Secretary of Defense and it required them to report on their progress in implementing the CDIP tasks. While the Deputy Secretary of Defense did require DOD components to implement these four tasks and report on their progress, components have not achieved performance targets. If DOD components do not develop plans with scheduled completion dates to implement the remaining four CDIP tasks, the department may fail to remove preventable, well-known vulnerabilities from its network and may allow adversaries to compromise the confidentiality, integrity, or availability of sensitive information and information systems.

[37]Endpoint security solutions are safeguards implemented through software to protect end-user machines (e.g., workstations and laptops) against attack. These safeguards can include antivirus, antispyware, anti-adware, personal firewalls, and host-based intrusion detection and prevention systems.

[38]GAO, *Information Technology: Agencies Need to Develop Modernization Plans for Critical Legacy Systems*, GAO-19-471 (Washington, D.C.: June 11, 2019). We also noted that, in some cases, vendors no longer provide support for hardware or software, creating cybersecurity vulnerabilities and additional costs.

DOD Does Not Know the Extent that Seven CDIP Tasks Have Been Implemented

DOD does not know the extent to which components have implemented the seven CDIP tasks that the CIO does not oversee because the responsible components have not reported on their progress, according to DOD officials. For example, DOD has not reported on the extent to which components have disabled hyperlinks to websites that users receive in email messages.[39] Disabling hyperlinks in email messages can help to prevent phishing attacks.[40] DISA officials told us that the agency implemented a security protocol that disables these hyperlinks in DISA's email server. Consequently, DOD components that use DISA's email service are compliant with this task's requirement; however, not all DOD components use DISA's email service and the extent to which other email services comply with this task is unknown.

The CDIP memorandum signed by the Deputy Secretary of Defense stated that the department's progress in implementing all CDIP tasks would be reported. However, the department has not reported on the progress it has made implementing the seven CDIP tasks that the CIO does not oversee in part because the Deputy Secretary of Defense did not identify, in the CDIP memorandum, a component to oversee the implementation of these tasks and report on their progress.

According to DOD CIO officials, some of these seven tasks are more tactical and may be more appropriately tracked at echelons below the office of the DOD CIO. For example, one of these seven tasks requires that commanders ensure the physical security of their network infrastructure devices. We agree that lower echelons may more effectively track the progress of some tasks; however, information about the progress that components make implementing these tasks is not reported to the CIO or any other DOD component, according to DOD officials. In addition, DOD CIO officials told us that JFHQ-DODIN collects some information from inspections it performs to verify the extent that inspected units implement technical guidance documents, some of which

[39]A hyperlink is text or a photo in a document or webpage that when clicked, connects to another webpage, section, or document.

[40]Phishing is a digital form of social engineering that uses hyperlinks, among others, in authentic-looking, but fake, emails to direct users to fake websites that request sensitive information (e.g., username and password) and download malware (i.e., malicious software intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system).

relate to these seven CDIP tasks. However, according to DOD officials, JFHQ-DODIN does not report this information to the CIO or any other DOD component. In addition, JFHQ-DODIN inspects a sample of DOD units and therefore does not have information about the status of these tasks across the department. For those units that are inspected, no DOD component is aggregating data from these inspections to identify the extent to which these seven tasks are implemented.

If the Deputy Secretary of Defense does not identify a DOD component to oversee the implementation of the seven CDIP tasks that DOD CIO does not oversee and report on progress implementing them, the department will have less assurance that cybersecurity vulnerabilities are being addressed in a timely manner and systems are being securely configured.

DOD Has Not Fully Implemented Its Cyber Awareness Challenge Training Initiative

Selected DOD Components Did Not Know the Extent to Which Their Users Implemented the 2018 Cyber Awareness Challenge Training

The 16 selected components we included in our sample did not always collect information on the number of users (1) that completed the fiscal year 2018 Cyber Awareness Challenge training, (2) that did not complete the training, and (3) whose network access was revoked for not completing the cyber awareness training. Specifically:

- **Unknown number of users that *completed* the cyber awareness training.** Two of the 16 did not collect information on the number of users that completed the fiscal year 2018 Cyber Awareness Challenge training. In particular, the Army and the Defense Finance and Accounting Service could not provide data on the extent that users had taken the required training in fiscal year 2018.
- **Unknown number of users that did *not complete* the cyber awareness training.** Six of the 16 components did not collect information on the number of users that did not complete the cyber awareness training. In particular, the Navy, Air Force, Marine Corps, U.S. European Command, and the Defense Media Activity did not collect information on the users who did not complete the training in fiscal year 2018. In addition, the Army's training compliance system did not have records for all Army users in 2018, which limited the

Army's ability to determine if all of its users completed the fiscal year 2018 Cyber Awareness Challenge training.

- **Unknown number of users whose network access had been revoked for not completing the required training.** Eight of the 16 components that we contacted did not collect data on the number of users whose network access had been revoked for not completing the required training, as implied by DOD policy.

Selected DOD components did not know the extent to which their network users implemented the 2018 Cyber Awareness Challenge training by completing it because the DOD component heads did not ensure that their respective components were accurately monitoring and reporting the necessary information. Navy officials told us that they believed it was not DOD or the military service's policy for the service headquarters to track whether their network users had completed the training. According to Navy officials, there is also no value for large organizations like the Navy, with over 600,000 users, to track and report these data at the headquarters level.

However, DOD policy requires all network users to take the Cyber Awareness Challenge training annually.[41] In addition, DOD policy states that all individuals with network access must complete this training to retain access. NIST also advises that agencies capture training compliance data at an agency level, so data can be used to conduct agency-wide analysis and reporting.[42]

Multiple DOD policy and guidance documents—including DOD Manual 8570.01-M, and Chairman of the Joint Chiefs of Staff Instruction 6510.01F—state that the DOD component heads are responsible for ensuring that users complete the Cyber Awareness Challenge training and two of these documents require recording training compliance. For example, according to DOD Manual 8570.01-M, *Information Assurance (IA) Workforce Improvement Program,* components must document and maintain the status of awareness compliance for each user.

[41]DOD 8570.01-M, *Information Assurance Workforce Improvement Program*; and CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND).* Authorized users of DOD information systems are required to receive initial IA orientation as a condition of information system access upon assignment to an organization and must complete DOD awareness training annually thereafter to maintain access.

[42]NIST Special Publication 800-50.

Further, service policy and guidance places the responsibility on the DOD component heads or senior-level leaders at the headquarters' level for ensuring that cybersecurity training is completed and documented. For example, Secretary of Navy Instruction 5239.3C, *Department of Navy Cybersecurity Policy* (May 2, 2016), states that the Chief of Naval Operations and the Commandant of the U.S. Marine Corps shall ensure all authorized users of Department of Navy information systems and networks receive initial cybersecurity awareness orientation as a condition of access and, thereafter, complete annual refresher training, monitor and report workforce cybersecurity training and maintain supporting records. Similarly, Army Regulation 25-2, *Army Cybersecurity* (Apr. 4, 2019), states that the Deputy Chief of Staff, G3/5/7 is responsible for ensuring that cybersecurity training is integrated and conducted throughout the Army.

If the DOD component heads do not ensure that their respective components accurately monitor and report information on the extent that users have completed the Cyber Awareness Challenge training—as well as have access revoked for not completing the training—the components may be unable to ensure that DOD users are trained in the steps needed to address cybersecurity threats to the department.

DARPA Has Not Required its Users to Take DOD's Cyber Awareness Challenge Training

One of the 16 selected components in our review—DARPA—did not require its users to take DOD's Cyber Awareness Challenge training, according to DARPA officials, even though it is required by policy.[43] Instead, DARPA has required its users to take cybersecurity training that it developed. While DARPA developed its own training program, we found that this training program did not address all of the requirements identified in a DOD staff manual or the cybersecurity training topics identified by the Cyber Workforce Advisory Group.[44] DARPA officials recognized that its cybersecurity training was not equivalent to the DOD's Cyber Awareness Challenge training program, which according to DOD CIO officials, addressed the training topics identified by the DOD Cyber Workforce Advisory Group. They explained that DARPA designs its courses to be concise to allow their personnel to focus on accomplishing the agency's

[43]DOD 8570.01-M.

[44]DOD 8570.01-M.

mission and that users can obtain additional information from references cited in the course materials. In addition, these officials told us that they were unaware their users were required to take the Cyber Awareness Challenge training that DISA developed.[45]

The DOD CIO is responsible for overseeing the implementation of the Cyber Awareness Challenge training, according to DOD CIO officials. However, DOD CIO officials told us they were not aware that DARPA has not required its users to take the Cyber Awareness Challenge training that DISA developed and they did not assess the extent that components complied with the requirement for components to use the DISA-developed training. If the DOD CIO does not ensure that DARPA and any other DOD components take the Cyber Awareness Challenge training developed by DISA, users in these components may take actions that lead to or enable exploitations of DOD information systems.[46]

DOD Does Not Know the Extent that Cyber Hygiene Practices Have Been Implemented to Protect DOD Networks from Key Cyberattack Techniques

DOD identified key techniques that adversaries use most frequently and that pose significant risk to the department's networks and identified cyber hygiene practices to protect the department's networks from these techniques. Specifically, JFHQ-DODIN has identified the cyberattack techniques that the agency observes adversaries using most frequently to attack the department's networks. In addition, the National Security Agency, the Defense Information Systems Agency, and the DOD CIO identified 177 cyberattack techniques and prioritized the techniques according to the level of risk each posed to the department's networks. The agencies prioritized the techniques using various criteria including the prevalence of the technique and whether the department could detect the use of the technique. Further, the department has established cyber hygiene practices to mitigate most of the frequently occurring techniques

[45]Since 2004, DISA has conducted multiple cybersecurity related inspections of DARPA and did not provide feedback indicating that the training that DARPA required its users to complete was an area of concern, according to agency officials.

[46]We focused our review on collecting information from 16 of DOD's 47 components. While DARPA was the only DOD component in our sample of 16 components that did not require its users to take the training that DISA developed, other components not in our sample may or may not require their users to take the DISA-developed training.

and those that the department identified as the highest priority, according to DISA and JFHQ-DODIN officials.

However, the department does not know the extent that these cyber hygiene practices have been implemented across the department to protect its networks from these key cyberattack techniques.[47] Components have visibility of the extent that they have implemented practices within their component, according to DOD officials. For example, DISA officials told us that they require their component to implement cyber hygiene practices to protect DOD networks from key cyberattack techniques and are able to determine the extent that those practices are implemented within DISA. However, no component or office within the department has complete visibility of the department's efforts to implement these protective practices across the department, according to DOD officials.

FISMA states that agency heads shall be responsible for, among other things, providing information security protections commensurate with the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification or destruction of such information systems.[48] Executive Order 13800 states that agency heads will be held accountable for managing cybersecurity risk to their enterprises.[49] The order requires agency heads to use the NIST's *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as the NIST Cybersecurity Framework) to manage their agency's cybersecurity risk.[50] The Cybersecurity Framework calls for senior executives to monitor cybersecurity risk in the same context as financial risk and other organizational risks. In doing so, the Cybersecurity Framework calls for

[47]For purposes of this report, we identified key techniques that adversaries use most frequently and that pose significant risk to the department's networks by assessing two DOD sources: (1) a list provided by JFHQ-DODIN that identified a subset of cyberattack techniques that the agency observed adversaries using most frequently in January 2019; and (2) a 2016 review conducted by the National Security Agency, the Defense Information Systems Agency, and the DOD CIO. We selected cyberattack techniques that the agencies identified as the highest priority. See appendix I for more information about how these techniques were identified.

[48]44 U.S.C. § 3554(a)(2)(A).

[49]Exec. Order No. 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, 82 Fed. Reg. 22,391 (May 16, 2017).

[50]National Institute for Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity* (commonly referred to as the NIST Cybersecurity Framework) (version 1.1, Apr. 16, 2018).

agencies to, among other things, assess cybersecurity risks (including threats), prioritize cybersecurity outcomes and requirements based on that risk, and establish processes to assess and monitor the implementation of the cybersecurity outcomes and requirements.

The department does not know the extent that practices to protect DOD networks from key cyberattack techniques have been implemented across the department in part because no DOD component monitors the extent to which such practices are implemented, according to DOD officials. Officials from JFHQ-DODIN told us that they are able to detect when adversaries are using techniques to attack the department's networks. However, detecting an attack after it has commenced may still enable an adversary to inflict harm on the department's networks and the information therein. If the Secretary of Defense does not direct a component to monitor the extent to which practices to protect its network are implemented, gaps in protection could go undetected. These gaps can jeopardize military operations, performance of critical functions, and protection of information within DOD systems and networks.

Senior DOD Leaders Have Not Received Information on Two Cyber Hygiene Initiatives or Cyber Hygiene Practices

DOD requirements and best practices recognize that senior DOD leaders need key information to make risk-based decisions. Specifically, the DC3I memorandum requires the commander of U.S. Cyber Command, in coordination with the DOD CIO, to provide quarterly updates to the Deputy Secretary of Defense and the Vice Chairman of the Joint Chiefs of Staff on the progress in implementing the DC3I. Further, the CDIP memorandum requires the department to report progress implementing the CDIP tasks. In addition, NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program,* states that the CIO should ensure that agency heads and senior managers are informed of the progress of the security awareness and training program's implementation.[51]

Senior DOD leaders receive two recurring reports on the department's cybersecurity posture that include information on one cyber hygiene

[51]NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program* (October 2003).

initiative. Specifically, the Cyber Hygiene Scorecard (Scorecard) is a report measuring compliance with DOD cybersecurity policies, procedures, standards and guidelines. The Scorecard provides information to the Secretary of Defense, the Deputy Secretary of Defense, and DOD component heads about the extent that the 10 CDIP tasks overseen by the DOD CIO are implemented. In addition, the Cyber Landscape Report is a quarterly report that includes information highlighting cybersecurity risks to DOD networks, U.S. critical infrastructure, DOD weapon systems, the cloud, and DOD's cyber workforce. Based on our analysis, the Cyber Landscape Report also includes some information from the CDIP initiative.

However, senior DOD leaders have not received information on the other two cyber hygiene initiatives or cyber hygiene practices to protect DOD networks from key cyberattack techniques in these recurring reports. Specifically, neither the Scorecard nor the Cyber Landscape Report includes information on the extent that the DC3I and the Cyber Awareness Challenge training have been implemented. In addition, neither of these recurring reports identifies key cyberattack techniques the department faces nor do they include information on the extent that the department has implemented cyber hygiene practices to protect DOD networks from these techniques, according to DOD officials.

Senior DOD leaders are not receiving complete information in part because the DOD CIO has not assessed the extent that the missing information could improve senior leaders' ability to make risk-based decisions. According to DOD officials, DOD CIO has not revised the recurring reports or developed a new report in response to such an assessment. DOD CIO officials told us that they do not believe that senior DOD leaders need to be made aware of all cyber hygiene topics we describe here—and in some cases that information could be managed at lower echelons within the organization. While some cyber hygiene information could be managed by lower-echelon DOD leaders, the DC3I memorandum requires information about its progress to be reported to senior leaders. The NIST guidance calls for similar reporting.

Additionally, a DOD official told us that the department uses the Cyber Hygiene Scorecard to respond to the department's requirement to annually report progress on implementing its information security program

to the Office of Management and Budget under FISMA.[52] Further, these officials told us that the Scorecard was not originally designed to include the information from our analysis such as information about the DC3I. They told us that this Scorecard was designed to provide an oversight tool to monitor the progress components made implementing the CDIP tasks overseen by DOD CIO.

However, while DOD uses the Scorecard with the intention to meet the FISMA annual reporting requirement, the Scorecard does not provide information about 53 of the 69 risk-management FISMA indicators that are called for by the Office of Management and Budget.[53] In addition, DOD CIO is not precluded from revising the Scorecard to include additional information. As one of two recurring reports sent to senior DOD leaders, the Cyber Hygiene Scorecard may be well positioned to provide additional information reflecting progress made implementing cyber hygiene initiatives and associated cybersecurity practices, including the DC3I and efforts to protect DOD networks from the key cyberattack techniques used by adversaries.

Further, a DOD CIO official told us that its officials did not include information about the DC3I in the Cyber Hygiene Scorecard because they believed it would be challenging to measure the culture-related objectives

[52]DOD provides the Scorecard as part of its FISMA reporting package. This package also includes an agency letterhead detailing the relevant information systems policies and any breaches or incidents reported, the DOD Senior Agency Official for Privacy report, which includes a privacy impact assessment and DOD's privacy policy, and the DOD Inspector General (IG) report.

[53]Department of Homeland Security, *Fiscal Year 2019 CIO FISMA Metrics, version 1* (December 2018). FISMA metrics are designed to assess agencies' progress in achieving outcomes that strengthen federal cybersecurity and provide the Office of Management and Budget a means to monitor agencies' progress toward implementing the President's priorities. Our analysis identified that the Cyber Hygiene Scorecard included information that was consistent with 16 of the fiscal year 2019 CIO FISMA metrics. The 16 FISMA metrics are: systems with security authorization to operate; number of devices assessed for vulnerabilities; number of government furnished equipment assets with each operating system; common security configuration baseline for each operating system; unprivileged users; privileged users; high value assets systems that require users to authenticate through two-factor personal identity verification; number of high value asset systems with automated mechanism for flaw remediation; number of unresolved vulnerabilities; number of endpoints covered by intrusion prevention system; number of endpoints covered by antivirus solution; number of endpoints covered by capacity to protect memory from unauthorized code execution; number of endpoints protected by tool to block known phishing websites; number of assets scanned for malware prior to remote access connection; percent of unclassified network that implemented solution to alert and detect connection of unauthorized hardware; and number of endpoints covered by software asset management capability.

in the DC3I. While the DC3I's culture-related objectives may be difficult to measure, the extent to which assigned DOD components have taken actions to implement the DC3I tasks is measurable. If the DOD CIO does not assess the extent that the missing information could improve senior leaders' ability to make risk-based decisions—and does not follow up to revise the recurring reports or develop a new report—senior DOD leaders will not be positioned well to make effective and risk-based decisions and manage cybersecurity risks.

Conclusions

As DOD has become increasingly reliant on IT systems and networks to conduct military operations and perform critical functions, risks to these systems and networks have also increased because IT systems are often riddled with cybersecurity vulnerabilities—both known and unknown. These vulnerabilities and human error can facilitate security incidents and cyberattacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security.

DOD has taken actions to address cyber vulnerabilities in the department through establishing the DC3I, the CDIP, the Cyber Awareness Challenge training, and cyber hygiene practices to protect its networks from cyberattack techniques that adversaries may use. However, the department faces challenges implementing the DC3I and CDIP because the DOD CIO has not taken appropriate steps to ensure that the DC3I tasks are implemented, DOD components have not developed plans with scheduled completion dates to implement the remaining four CDIP tasks overseen by DOD CIO, and the Deputy Secretary of Defense has not identified a DOD component to oversee the implementation of the seven other CDIP tasks and report on progress implementing them. By improving oversight through implementing the DC3I tasks, DOD components developing plans with scheduled completion dates to implement the remaining four CDIP tasks that the DOD CIO oversees, and identifying a DOD component to oversee implementation of the seven other CDIP tasks and report on progress implementing them, the department can be better positioned to safeguard DOD's network by removing preventable, well-known vulnerabilities.

If the components address gaps we identified in the extent that they account for whether their users completed the 2018 Cyber Awareness

Challenge training will help the department gain assurance that its workforce is prepared to identify and appropriately respond to cybersecurity risks. Additionally, by ensuring that DARPA, and any other similar DOD components, requires its users to take the required DISA-developed training, DOD users may be more aware of threats and vulnerabilities to the department's networks and may be better equipped to prevent exploitations of DOD information systems.

The department does not know the extent that cyber hygiene practices have been implemented to protect DOD networks from key cyberattack techniques. By directing a component to monitor the extent to which practices to protect DOD's networks are implemented, DOD would be better positioned to ensure that its networks are secure and decrease potential risks to military operations, critical functions, and information assurance.

Finally, the lack of information on two cyber hygiene initiatives and cyber hygiene practices in recurring reports provided to senior DOD leaders is concerning because of the need for those leaders to have a complete picture of the state of the department's cybersecurity posture. By directing DOD CIO to assess the extent that the missing information could improve senior leaders' ability to make risk-based decisions and revise the recurring reports or develop a new report, DOD leaders would then be better positioned to make effective decisions and manage cybersecurity risks.

Recommendations for Executive Action

We are making seven recommendations to the Department of Defense.

The Secretary of Defense should ensure that the DOD CIO takes appropriate steps to ensure implementation of the DC3I tasks. (Recommendation 1)

The Secretary of Defense should ensure that DOD components develop plans with scheduled completion dates to implement the four remaining CDIP tasks overseen by DOD CIO. (Recommendation 2)

The Secretary of Defense should ensure that the Deputy Secretary of Defense identifies a DOD component to oversee the implementation of

the seven CDIP tasks not overseen by DOD CIO and report on progress implementing them. (Recommendation 3)

The Secretary of Defense should ensure that DOD components accurately monitor and report information on the extent that users have completed the Cyber Awareness Challenge training as well as the number of users whose access to the network was revoked because they have not completed the training. (Recommendation 4)

The Secretary of Defense should ensure that the DOD CIO ensures all DOD components, including DARPA, require their users to take the Cyber Awareness Challenge training developed by DISA. (Recommendation 5)

The Secretary of Defense should direct a component to monitor the extent to which practices are implemented to protect the department's network from key cyberattack techniques. (Recommendation 6)

The Secretary of Defense should ensure that the DOD CIO assesses the extent to which senior leaders' have more complete information to make risk-based decisions—and revise the recurring reports (or develop a new report) accordingly. Such information could include DOD's progress on implementing (a) cybersecurity practices identified in cyber hygiene initiatives and (b) cyber hygiene practices to protect DOD networks from key cyberattack techniques. (Recommendation 7)

Agency Comments and Our Evaluation

We provided a draft of this report to the department for review and comment. In written comments, reprinted in appendix III, DOD concurred with one of our seven recommendations, partially concurred with four, and did not concur with the remaining two. DOD separately provided technical comments, which we incorporated as appropriate.

The department concurred with our recommendation (Recommendation 5) that the DOD CIO ensure all components, including DARPA, require their users to take the Cyber Awareness Challenge training developed by DISA.

The department partially concurred with four of our recommendations.

- The department partially concurred with our recommendation that the DOD CIO take steps to ensure that DC3I tasks are implemented. The department concurred that tasks two and six in the DC3I should be implemented and stated that these two tasks are the only two still actively being pursued. The department stated that the remaining five tasks were either implemented or have been overcome by events. However, the department did not provide evidence that the other five tasks were implemented or demonstrate how these tasks were overcome by events during the audit or in its comments on a draft or our report. In addition, JFHQ-DODIN officials stated that the principles outlined in the DC3I are important for the department to achieve its cybersecurity goals. For example, several of these five tasks were focused on improving cybersecurity awareness and training at all levels within the department. Therefore, it is unclear why DOD believes that these cyber hygiene tasks have been overcome by events; DOD did not elaborate. Implementing all seven DC3I tasks that have not been implemented can better position the department to achieve the goals of the DC3I to (1) mitigate the risks of compromising the confidentiality, integrity, and availability of mission-critical information as a result of human error by users on the department's networks; and (2) transform DOD cybersecurity culture by enabling and reshaping leaders, cyber providers, personnel who perform cyberspace operations, and general users to improve individual human performance and accountability on DOD's network.
- The department partially concurred with our recommendation that DOD components develop plans with scheduled completion dates to implement the four remaining CDIP tasks overseen by DOD CIO. DOD provided classified comments on this recommendation. Thus, we cannot respond in detail to their comments. We plan to respond to DOD's comments in a classified version of this report, which we plan to issue later in 2020. Developing plans that would facilitate implementation of these four CDIP tasks would better position DOD to meet the Deputy Secretary of Defense's goal of removing preventable vulnerabilities from DOD's network that could allow adversaries to compromise information and information systems.
- The department partially concurred with our recommendation that components accurately monitor and report information on the extent that users have completed the Cyber Awareness Challenge training and information on the number who have been denied access to the network for not completing the training. The department concurred that it should ensure components accurately report the number of users who have completed the training. However, it did not concur that components should report the number of users who have been

denied access to the network because they have not completed the training. The department stated that a statistic showing this information would not be meaningful and would be burdensome to collect. We disagree that such a measure would not be meaningful because it would help leaders hold network users accountable and better position DOD components to comply with DOD policy.[54] Recognizing that trained and aware users are the first and most vital line of defense, DOD components should document and maintain the status of awareness compliance for each user. In its current approach, DOD is unable to confirm whether all of its network users have completed the cybersecurity training, as required. For example, as stated above, 8 of the 16 (50 percent) of the DOD components we requested training information from told us they did not monitor whether users who did not complete the annual training were blocked from DOD networks and systems. If the Secretary of Defense does not ensure that DOD components accurately monitor and report information on the number of users whose access to the network was revoked because they have not completed the training, the components will jeopardize the department's ability to ensure that DOD users are trained in steps needed to address cybersecurity threats to the department.

In responding to this recommendation, DOD also stated that the Navy indicated that it provided us data on the number of its users who completed the training and the total number of its users. The department stated that we could compute the number of Navy users who had not completed the training by computing the difference between the total number of users and the number of users who completed the training. We updated our assessment of the Navy in our report. We now indicate that the Navy was able to identify the number of users who had completed the training in fiscal year 2018. However, we disagree that the difference between the total number of users and the number of users who completed the training equates to the number of users who did not take the training. DOD CIO officials told us during our audit that computing the number of users using this method is not reliable because there are multiple explanations for the difference between the total number of users and the number of users who took the training. For example, officials told us that some military users leave the service before they complete the

[54]See, for example, DOD 8570.01-M, *Information Assurance Workforce Improvement Program* and CJCSI 6510.01F, *Information Assurance (IA) and Support to Computer Network Defense (CND)*.

annually required training and are included in the service's total number of users but are not included in the number of users who took the training.

- The department partially concurred with our recommendation that the CIO assess the extent to which senior leaders have information to make risk-based decisions and then revise accordingly the recurring reports. The department stated that it will revise the recurring reports by merging the Cyber Hygiene Scorecard and a scorecard related to the Cyber Landscape to assist senior leaders' decision-making. However, the department stated that it did not fully agree with the recommendation because, as written in the draft report, the department believed the recommendation was stating that DOD should have "complete" information. Based on DOD's comment, we clarified the recommendation to state that senior DOD leaders should have more complete information to make risk-based decisions. We believe this is critical because the cyber hygiene tasks and practices highlighted in the report were identified by the most senior leaders in the department—including the Secretary of Defense, Deputy Secretary of Defense, and Chairman of the Joint Chiefs of Staff—as being the tasks and practices that were essential to protecting DOD information, systems, and networks from the most common and pervasive cybersecurity risks faced by the department. The department also stated that risk is a function of multiple variables, that are continually evolving. We agree that risk is a function of multiple variables—including threats and vulnerabilities—that are continually evolving. As such, we think that information, such as the extent to which cyber hygiene practices have been implemented across the department to protect its networks from evolving key cyberattack techniques, will position senior leaders to make more effective and risk-based decisions and manage cybersecurity risks. The department did not concur with two recommendations. In particular:
- DOD did not concur with our recommendation that the Deputy Secretary of Defense identify a component to oversee the implementation of the seven CDIP tasks that the CIO does not oversee and report on progress implementing those tasks. The department stated that, since the CDIP's approval in 2015, the department has issued new or updated versions of a number of cyber-related strategies, including the DOD Cyber Strategy. The department also stated that the Deputy Secretary of Defense directed DOD to develop a classified top 10 list of cybersecurity critical-risk areas and an associated scorecard that provides the Deputy Secretary a quarterly assessment of the department's progress in reducing the risk for each of these areas. The department also stated that the

cyber landscape is constantly evolving with changes in technology, threats, and vulnerabilities, and that this requires DOD to reassess its cybersecurity priorities. The department stated that implementing our recommendation would override these recent efforts and focus the department's efforts on monitoring areas with lower levels of risk.

We disagree that implementing our recommendation would override the department's recent efforts. In fact, implementing the seven tasks would align with one of the 2018 DOD Cyber Strategy's objectives to "secure DOD information and systems against malicious cyber activity." We agree with DOD that the department should reassess cybersecurity priorities in light of changes in technologies, threats, and vulnerabilities. However, DOD did not provide evidence during the audit or in responding to the draft report that the department had assessed the CDIP tasks required by the Deputy Secretary of Defense in 2015. Specifically, the department has not determined whether they remain valid or aligned with the current cybersecurity threat environment, that the vulnerabilities associated with these seven tasks were mitigated or addressed, and that a senior-level DOD official provided written direction canceling the Deputy Secretary of Defense' CDIP taskings. More importantly, our analysis of the seven tasks that DOD is not currently tracking progress on are consistent with basic cybersecurity standards established by DOD guidance and NIST—and which DOD is planning to apply to certain defense contractors in future contract awards to protect DOD information that is stored or transits through their networks as a part of the Cybersecurity Maturity Model Certification framework.[55] For example,

- Task 14 requires commanders and supervisors to ensure physical security of their network infrastructure devices. This task aligns with general NIST guidance regarding physical access protections. NIST guidance states that organizations should manage and protect

[55]In January 2020, DOD issued the first version of a Cybersecurity Maturity Model Certification framework, which DOD plans to implement to assess and enhance the cybersecurity posture of certain defense contractors as a requirement for future contract awards. The framework will seek to assess cybersecurity maturity processes and cybersecurity best practices drawn from existing cybersecurity standards and other frameworks and references. The framework includes, among other things, 5 levels of cybersecurity best practices such as Level 1 "basic cyber hygiene"; Level 2 "intermediate cyber hygiene"; and, Level 3 "good cyber hygiene."

physical access to assets and facilities where information systems reside.[56]

- Task 15 requires commanders and supervisors to report all commercially provided internet connections to DOD's unclassified network. This task aligns with general NIST guidance regarding the use of external networks. NIST guidance states that organizations should catalogue all external information systems.[57]
- Task 16 requires commanders and supervisors to ensure alignment to a Computer Network Defense Service Provider. This task is consistent with DOD requirements on cybersecurity activities to protect the DOD Information Network. The requirements state that DOD IT must be aligned to DOD network operations and security centers, which provide any required cybersecurity services.[58]
- Task 17 requires commanders and supervisors with Computer Network Defense Service Provider responsibility to ensure the cyber incident response plan(s) are properly exercised and documented. This task aligns with general NIST guidance regarding incident response. NIST guidance states that organizations should provide incident response handling training and implement incident handling capabilities, as well as a process to ensure that response processes and procedures are executed, and maintained ensuring response to detected cybersecurity incidents.[59]

If the Deputy Secretary of Defense does not implement this recommendation, the department will have less assurance that

[56]NIST SP 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), PE-3, Physical Access Controls, states that organizations manage physical access to facilities where information systems reside. In addition, NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Apr. 16, 2018) PR.AC-2 states that physical access to assets should be managed and protected.

[57]NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Apr. 16, 2018) PR.AC-3 states that organizations should manage remote access and ID.AM-4 states that organizations should catalogue external information systems.

[58]Department of Defense Instruction 8530.01*, Cybersecurity Activities Support to DoD Information Network Operations* (Mar. 7, 2016).

[59]NIST SP 800-53 Rev. 4 *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013) IR-2 and IR-4 state that organizations should provide incident response training and implement incident handling capabilities. NIST, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1* (Apr. 16, 2018) RS.RP states organizations should ensure that response processes and procedures are executed and maintained to ensure response to detected cybersecurity incidents.

cybersecurity vulnerabilities are being addressed in a timely manner and systems are being securely configured.

- The department did not concur with our recommendation that a component monitor the extent of implementation of practices to protect the department's network from key cyberattack techniques. The department determined that the information in its response to this recommendation included sensitive information. Therefore, we are redacting the department's response to this recommendation from DOD's written comments that we are reprinting in Appendix III. However, we still believe the recommendation is valid. As stated in our report, no component or office within the department has complete visibility of the department's efforts to implement these protective practices across the department, according to DOD officials. Taking action to implement the intent of this recommendation would help address that gap.

We are sending copies of this report to the appropriate congressional committees; the Secretary of Defense; DOD's Chief Information Officer; the Secretaries of the Army, Navy, and Air Force; the Commandant of the Marine Corps; the Chairman of the Joint Chiefs of Staff; the Commanding Generals of U.S. Strategic Command, U.S. European Command, U.S. Southern Command, and U.S. Cyber Command; and the Directors of DISA, the National Security Agency, DARPA, the Defense Commissary Agency, the Defense Contract Management Agency, the Defense Finance and Accounting Service, the Defense Media Activity, and the Defense Technology Security Administration. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact us: Joseph Kirschbaum at (202) 512-9971 or kirschbaumj@gao.gov, or Nick Marinos at (202) 512-9342 or marinosn@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.

Joseph W. Kirschbaum
Director, Defense Capabilities and Management

Nick Marinos
Director, Information Technology and Cybersecurity

List of Committees

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

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

The Honorable Adam Smith
Chairman
The Honorable Mac Thornberry
Ranking Member
Committee on Armed Services
House of Representatives
The Honorable Pete Visclosky
Chairman
The Honorable Ken Calvert
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

Appendix I: Scope and Methodology

For the purposes of this review, we adapted a definition of cyber hygiene developed by Carnegie Mellon University's Software Engineering Institute. The institute defines cyber hygiene as a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today.[1]

We discussed the definition of cyber hygiene with Department of Defense (DOD) officials to identify DOD initiatives aimed at improving cyber hygiene. DOD officials identified the Cyber Discipline Implementation Plan (CDIP) as DOD's main cyber hygiene initiative aimed at implementing technical improvements to DOD networks. In addition, DOD officials identified the DOD Cybersecurity Culture and Compliance Initiative (DC3I) and DOD's Cyber Awareness Challenge training as two initiatives designed to establish best practices for DOD network users including military personnel, civilians, and contractors.

To determine the extent to which DOD has implemented its three cyber hygiene initiatives and practices to protect its networks from cyberattack techniques that adversaries may use, we conducted analyses for each initiative.

- To determine the extent to which DOD implemented the DC3I, we reviewed the 11 tasks that require components to take actions that are specified in the DC3I memorandum that the Secretary of Defense and the Chairman of the Joint Chiefs of Staff issued in September 2015.[2] We analyzed documentation we collected from U.S. Cyber Command, the office of the DOD Chief Information Officer (CIO), and the Joint Staff that demonstrate actions these components took in response to each of the 11 DC3I tasks and determined the extent to which each task was implemented.

[1]Carnegie Mellon University Software Engineering Institute, *Cyber Hygiene: A Baseline Set of Practices* (2017).

[2]Secretary of Defense and Chairman of the Joint Chiefs of Staff Memorandum, *Department of Defense Cybersecurity Culture and Compliance Initiative* (Sept. 30, 2015).

- To determine the extent to which DOD implemented the CDIP, we reviewed the 17 tasks that require components to take actions specified in a memorandum that the Deputy Secretary of Defense issued in October 2015.[3] We interviewed officials from the office of the DOD CIO about the extent to which DOD components implemented the CDIP tasks, the reasons the components had not fully implemented all of the tasks, and to determine the extent that the DOD CIO knew if DOD components had implemented the remaining seven CDIP tasks. We also reviewed documentation on the extent that DOD components implemented the tasks overseen by DOD CIO by analyzing data included in the Cyber Hygiene Scorecard. We also assessed the reliability of the data in the Scorecard by reviewing the methods the DOD CIO uses to ensure the data reported to the Scorecard are accurate and interviewing cognizant officials. We determined the data are sufficiently reliable for our purposes.
- To determine the extent that DOD implemented the Cyber Awareness Challenge training, we analyzed the extent that the DOD CIO and the DOD component CIOs ensured that personnel they oversee completed the fiscal year 2018 Cyber Awareness Challenge training. To carry out this analysis, we collected and analyzed information from the DOD CIO and a sample of 16 DOD components.

We selected this sample of components by identifying important groupings of components and selecting from these groups to ensure that our sample represented a significant number of DOD personnel as well as a variety of types of components. These groups were: the military services and the Joint Staff, combatant commands, agencies and field activities, and the Office of the Secretary of Defense.

- **Military services and Joint Staff.** We selected the four military services because they are the components within DOD with the most personnel. We also included the Joint Staff because this component reflects the strategic perspective for the department as a whole.
- **Combatant commands.** We randomly selected three combatant commands from the group of 11 combatant commands—including geographic (e.g., U.S. Central Command) and functional (e.g., U.S. Transportation Command). We selected three of the 11 combatant commands to include the perspectives of multiple combatant commands in our sample. We selected these combatant commands:

[3]Deputy Secretary of Defense Memorandum, *DOD Cybersecurity Campaign–Cybersecurity Discipline Implementation Plan* (Oct. 26, 2015).

U.S. European Command, U.S. Southern Command, and U.S. Strategic Command.

- **Agencies and Field Activities.** We assembled a list of non-service and non-combatant command components organized by the types of functions that each component performs. We then organized these components by functional groupings. Specifically, we created functional groupings for the components that fall under each of the six Under Secretaries of Defense because these officials oversee components with similar functions.[4] We also included a seventh functional group of miscellaneous components that are not overseen by any of the Under Secretaries of Defense. We then accounted for the size of the components on this list by identifying the larger agencies and the smaller field activities. From this list, we randomly selected one component from each of the seven groups. In doing so, we selected five of the 20 agencies and two of the eight field activities. We chose this ratio of agencies to field activities to reflect the ratio of agencies to field activities in DOD. That is, DOD agencies are about 71 percent of DOD's non-service and non-combatant command components and about 71 percent of our sample.

  We selected these five agencies: Defense Advanced Research Projects Agency, Defense Commissary Agency, Defense Contract Management Agency, Defense Finance and Accounting Service and the National Security Agency. We selected these two field activities: Defense Media Activity and Defense Technology Security Administration.

- **The Office of the Secretary of Defense.** We also randomly selected one of 16 components from the Office of the Secretary of Defense. This group included the offices that support the six Under Secretaries we discussed above such as the Under Secretary of Defense for Policy as well as other offices including the Office of Cost Assessment and Program Evaluation and the Office of the DOD Chief Management Officer. We selected one component from this group to ensure we reflected the perspective of components at the DOD headquarters level. We selected the Office of the DOD Chief Information Officer.

To collect information from this sample of 16 components, we developed a standard set of questions we provided to each component on topics related to both objectives. In particular, we asked DOD components to provide the number of network users that completed the fiscal year 2018

[4]For example, the Under Secretary of Defense for Intelligence oversees five intelligence agencies such as the National Security Agency.

Cyber Awareness Challenge training, the number of network users that did not complete the training, and the number of network users who had their access to the network removed as a result of not taking the training. We also asked other questions including a question about the information that senior leaders are provided regarding cyber hygiene practices.

Each component provided written responses to our questions and in some cases provided documentation corroborating their responses. We conducted a content analysis of the components' responses and the documentation they provided. To complete this content analysis, two analysts assessed the components' responses, compared and discussed their separate analyses, and reached agreement on their conclusions about their analysis. We compared the information we collected from these components to a provision in NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program,* which advises agencies to capture training compliance data at an agency level.

Further, we interviewed officials from Defense Information Systems Agency and JFHQ-DODIN to determine the extent to which DOD had implemented cyber hygiene practices that the department has implemented to protect its networks from key cyberattack techniques that adversaries may use.

To determine the extent to which senior DOD leaders receive information on the department's efforts to address cyber hygiene initiatives and practices, we first defined senior DOD leaders as the Secretary of Defense, the Deputy Secretary of Defense, and DOD component heads. To identify the information that could be included in reports that senior DOD leaders receive about DOD efforts to mitigate cyberattack techniques, we identified techniques that are most likely to be used by adversaries against DOD's networks or that could cause severe adverse effects on DOD's operations. In particular, we identified 22 key cyberattack techniques from two sources:

- Joint Force Headquarters DOD Information Network (JFHQ-DODIN) provided a list of eight cyberattack techniques that the agency observed adversaries using most frequently in January 2019.[5] JFHQ-

[5]JFHQ-DODIN provided data on the most frequent attack techniques that adversaries used to attack DOD networks during January 2019. These data represent the most commonly observed threat tactics DOD faces beyond the month of January 2019, according to JFHQ-DODIN officials.

DODIN officials also determined that these data are representative of the cyberattack techniques that they have recently observed.

- We identified 14 cyberattack techniques by analyzing a review conducted in 2016 by the National Security Agency, the Defense Information Systems Agency, and the DOD CIO. In the review, the agencies identified 177 cyberattack techniques and ranked the techniques according to the level of risk the techniques posed to DOD's unclassified and Secret-level networks.[6] The agencies used a number of different criteria to rank these techniques, including the prevalence of the technique, visibility of the technique, and whether other, closely associated alternative techniques exist. We selected the 14 cyberattack techniques that the agencies identified as the highest priority.

Next, we analyzed the contents of two recurring reports that senior leaders receive on the department's cybersecurity posture: the Cyber Hygiene Scorecard and the Cyber Landscape Report. In particular, we analyzed these reports to determine if they included information about DOD's implementation of key cyber hygiene initiatives that we describe in the first objective. We also analyzed the reports to determine if they included the lists of key cyberattack techniques and information about the extent that the department had implemented cyber hygiene practices to protect DOD networks from these cyberattack techniques.

We conducted this performance audit from January 2019 to April 2020 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.

[6]DOD CIO, NSA, and DISA *NIPRNet/SIPRNet Cybersecurity Architecture Review* (December 2016).

Appendix II: DOD Cybersecurity Culture and Compliance Initiative Tasks

The Department of Defense (DOD) Chief Information Officer (CIO) and other relevant DOD components implemented four of the 11 tasks required in the Cybersecurity Culture and Compliance Initiative (DC3I) and the remaining seven tasks were not fully implemented as of October 2019. Table 2 provides additional information of actions taken to address and implement all 11 DC3I tasks.

Table 2: Our Assessment of the Implementation Status of DOD Cybersecurity Culture and Compliance Initiative (DC3I) Tasks

Tasks	Our Assessment of the Implementation Status	Description of the Implementation Progress as of October 2019
1: U.S. Cyber Command will develop cybersecurity training briefs for combatant commanders, services, agencies, and all other DOD components to use in leadership training.	Not Fully Implemented	U.S. Cyber Command developed two training briefings for DOD leadership. However, as of October 2019, neither U.S. Cyber Command nor the Office of the DOD CIO had disseminated these leadership training briefs across the department, according to DOD officials.
2: U.S. Cyber Command and the DOD Chief Information Officer (CIO) direct the appropriate stakeholders to develop educational and training requirements for cyber providers.	Not Fully Implemented	DOD CIO has not developed educational and training requirements for cyber providers. According to the DOD CIO, the office is revising DOD Manual 8140, *Cyber Workforce Qualification and Management Program,* which documents educational and training requirements for DOD's cyber workforce. DOD CIO officials stated that the manual is expected to be complete around April 2020.
3: DOD CIO will implement scenario-based training to educate users on potential mission impacts as a result of failures to follow cybersecurity procedures.	Implemented	In October 2016, the Defense Information Systems Agency (DISA) implemented scenario-based training into the Cybersecurity Awareness Challenge training.
4: Combatant commanders, service chiefs, agency, and DOD component heads will take appropriate actions to incorporate the DC3I principles into all levels of training.	Not Fully Implemented	No action for this task can be taken until DOD components receive deliverables from tasks 1 and 2. DOD CIO officials said that this task will be implemented, in part, through dissemination of educational and training requirements for cyber providers that are expected to be complete around April 2020.

Tasks	Our Assessment of the Implementation Status	Description of the Implementation Progress as of October 2019
5: Chairman Joint Chiefs of Staff will develop and implement criteria for assessing combatant commander and military service efforts to integrate cybersecurity into operational training and exercises.	Not Fully Implemented	Joint Staff developed criteria for assessing cybersecurity integration into operational training and exercises. In May 2016, Joint Staff Vice Chairman directed integration of the criteria into Chairman of the Joint Chiefs of Staff Notice 3500.01, *Chairman's Joint Training Guidance*. However, Joint Staff officials told us the criteria was never incorporated in this guidance. In September 2019, Joint Staff officials told us that these criteria will no longer be incorporated into CJCS Notice 3500.01, and Joint Staff will take no further action to implement this task.
6: U.S. Cyber Command and Joint Force Headquarters DOD Information Network (JFHQ-DODIN) will develop a resourcing plan to support scheduled inspections and no-notice spot checks.	Not Fully Implemented	JFQH-DODIN has not developed a resourcing plan to support cybersecurity inspections and spot checks. U.S. Cyber Command officials said a resourcing plan is in development and did not identify an expected completion date.
7: U.S. Cyber Command will promulgate the format and process for submitting quarterly reports from inspected units.	Implemented	In May 2016, U.S. Cyber Command provided guidance to JFHQ-DODIN on the format and process for submitting quarterly reports from inspected units. JFHQ-DODIN continues to send quarterly reports to U.S. Cyber Command that reflect observations and trends in inspections across inspected units.
8: U.S. Cyber Command will provide updated format and process for incident reporting.	Implemented	In April 2017, U.S. Cyber Command issued a task order directing DOD components to utilize an electronic tool managed by JFHQ-DODIN to report cyber incidents. The electronic tool specifies the format and process for DOD components to report cyber incidents.
9: U.S. Cyber Command and DOD CIO will lead an assessment and provide recommendations for the changes that need to be made to capabilities, authorities and network architectures.	Not Fully Implemented	U.S. Cyber Command led an assessment in coordination with 14 other DOD components and made five recommendations. In addition, U.S. Cyber Command identified offices of primary responsibly to take action in response to each recommendation. However, DOD CIO officials told us the office is not tracking implementation of these recommended actions.
10: U.S. Cyber Command and DOD CIO will lead the initial assessment and provide recommendations for what impact human resource shortfalls have on cyber provider missions and to recommend corrective actions to remedy these shortfalls.	Implemented	In April 2019 the office of the DOD CIO provided plans to address cyber work roles of critical need to the Office of Personnel Management. For example, the plan addresses cyber work role shortages through filling vacant positions, enhancing outreach and recruitment, and expanding on hiring authorities.

Tasks	Our Assessment of the Implementation Status	Description of the Implementation Progress as of October 2019
11: U.S. Cyber Command will provide an assessment and recommendations for what resources (dollars and people) are required to stand up the capability as the DC3I mission owner.	Not Fully Implemented	U.S. Cyber Command and DOD CIO have not assessed and recommended the required resources to implement the DC3I. In June 2016, U.S. Cyber Command completed an assessment to determine the DOD office best suited to take DC3I mission lead to transition DC3I efforts from an initiative to an enduring activity. In September 2016, U.S. Cyber Command recommended that the Deputy Secretary of Defense make DOD CIO the mission lead of the DC3I, and in December 2016 the Deputy Secretary of Defense assigned DOD CIO as DC3I mission lead. U.S. Cyber Command and the office of the DOD CIO could not provide any additional documentation that identifies required resources to implement the DC3I.

Source: GAO analysis of Department of Defense (DOD) information. | GAO-20-241

Appendix III: Comments from the Department of Defense

[redacted]

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

CHIEF INFORMATION OFFICER

MAR - 2 2020

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

Dear Mr. Kirschbaum:

(U) This is the Department of Defense (DoD) response to the GAO Draft Report, GAO-20-241, "CYBERSECURITY: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene," undated (GAO Code 103230). The Department concurs or partially concurs with portions of the draft report, and non-concurs with other portions. Enclosed are detailed comments on the report recommendations.

(U) The Department appreciates the opportunity to review the draft report. My point of contact for this matter is Mr. Kevin Dulany, kevin.m.dulany.civ@mail.mil, (571) 232-2850.

Sincerely,

/s/ Dana Deasy

Enclosure:
As stated

[redacted]

[redacted]

(U) GAO DRAFT REPORT, UNDATED, RECEIVED JANUARY 22, 2020 GAO-20-241 (GAO CODE 103230)

(U) "CYBERSECURITY: DOD NEEDS TO TAKE DECISIVE ACTIONS TO IMPROVE CYBER HYGIENE"

(U) DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

(U) RECOMMENDATION 1: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO takes appropriate steps to ensure that the DC3I tasks are implemented. (Recommendation 1)

(U) DoD RESPONSE: DoD partially concurs with Recommendation 1. DoD concurs that Task 2 and 6 should continue to be implemented. They are the only two tasks still being actively pursued because the remaining tasks were either implemented or have been overcome by events. Regarding Task 2, the re-issuance of DoD Directive 8140.01 is in the final stages of formal staffing and is expected to be released by October 2020, and will be followed by the later release of both DoD Instruction 8140.AB (new) and DoD Manual 8140. 01 (new - replaces/cancels DoDM 8570.01). Each one of these issuances are at different stages of development and coordination. The manual, which specifically addresses the cyber workforce education and training requirements, will be last to be published and is expected to take approximately 14 – 18 months to complete. Regarding Task 6, U.S. Cyber Command has indicated it is in the process of developing a resourcing plan to support scheduled inspections and no-notice spot checks.

(U) RECOMMENDATION 2: The GAO recommends that the Secretary of Defense should ensure that DOD components develop plans with scheduled completion dates to implement the four remaining Cyber Discipline Implementation Plan (CDIP) tasks overseen by DOD CIO. (Recommendation 2)

(U) DoD RESPONSE: DoD partially concurs with Recommendation 2. The unclassified report does not specifically identify the four tasks. We will reserve our detailed response for the classified version of the report.

(U) RECOMMENDATION 3: The GAO recommends that the Secretary of Defense should ensure the Deputy Secretary of Defense identifies a DOD component to oversee the implementation of the seven CDIP tasks and report on progress implementing them. (Recommendation 3)

(U) DoD RESPONSE: DoD non-concurs with Recommendation 3. The cyber landscape is constantly evolving with changes in technology, threats, and vulnerabilities. This requires DoD to reassess its cybersecurity priorities. Since the CDIP's approval in 2015,

[redacted]

1

[redacted]

the Department has issued new or updated versions of the National Defense Strategy, DoD Cyber Strategy, Digital Modernization Strategy, DoD Cloud Strategy, Artificial Intelligence Strategy, and is on the cusp of issuing a DoD Cybersecurity Risk Reduction Strategy. Further, the Deputy Secretary of Defense (DSD) directed DoD develop a classified Top 10 list of cybersecurity critical risk areas, which is subject to periodic review and update. The classified Top 10 Scorecard provides the DSD with a quarterly assessment of the Department's cybersecurity risk reduction progress in these areas. To require that all of this new strategic direction and prioritization be overridden to monitor compliance with lower risk areas that the DoD identified almost five years ago will frustrate the Department's efforts to keep pace with the changing tactics, techniques, and procedures of our adversaries and the evolving changes in technology.

(U) RECOMMENDATION 4: The GAO recommends that the Secretary of Defense should ensure that DOD components accurately monitor and report information on the extent that users have completed the Cyber Awareness Challenge training as well as the number who have access to the network revoked due to not completing the training. (Recommendation 4)

(U) DoD RESPONSE: DoD partially concurs with Recommendation 4. DoD concurs that it should ensure DoD components accurately report the number of users completing the required training. However, DoD non-concurs with the recommendation to report the number of users who have had network access temporarily revoked for non-compliance with the annual training requirement. The latter metric would not be meaningful but would be extremely burdensome to collect since network revocations can be for a variety of reasons and cross multiple networks and domains.

Contrary to the report's findings, the Navy indicates that it did provide GAO with the number of users completing the cyber awareness training and the total number of users, from which the number of users not completing the training could be computed.

(U) RECOMMENDATION 5: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO ensures that all DOD components, including DARPA, require their users to take the Cyber Awareness Challenge training developed by DISA. (Recommendation 5)

(U) DoD RESPONSE: Concur. DoD 8510.01-M currently requires the DISA-developed course be used to meet both the initial and annual awareness training mandated training.

(U) RECOMMENDATION 6: The GAO recommends that the Secretary of Defense should direct a component to monitor the extent to which practices to protect the department's network from key cyberattack techniques are implemented. (Recommendation 6)

[redacted]

2

[redacted]

[redacted]

(U) **RECOMMENDATION 7**: The GAO recommends that the Secretary of Defense should ensure that the DOD CIO assesses the extent to which senior leaders' have complete information to make risk based decisions-and revise the recurring reports (or develop a new report) accordingly. Such information could include DOD's progress on implementing 1) cyber hygiene initiatives and (2) cyber hygiene practices to protect DOD networks from key cyberattack. (Recommendation 7)

(U) **DoD RESPONSE**: DoD partially concurs with Recommendation 7. DoD concurs that it will revise the recurring reports by merging the Cyber Hygiene and Top 10 Scorecards to further assist senior leader decision-making by correlating the data in both scorecards. DoD non-concurs that it is possible to have "complete information to make risk-based decisions." Risk is a function of multiple variables and these variables are continually evolving. Timely, relevant, and correlated information is the best that can be expected.

[redacted]

3

Agency Comment Letter

Text of Appendix III: Comments from the Department of Defense

Page 1

March 2, 2020

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

Dear Mr. Kirschbaum:

(U) This is the Department of Defense (DoD) response to the GAO Draft Report, GA0-20- 241, "CYBERSECURITY: DOD Needs to Take Decisive Actions to Improve Cyber Hygiene," undated (GAO Code 103230). The Department concurs or partially concurs with portions of the draft report, and non-concurs with other portions. Enclosed are detailed comments on the report recommendations.

(U) The Department appreciates the opportunity to review the draft report. My point of contact for this matter is Mr. Kevin Dulany, kevin.m.dulany.civ@mail.mil, (571) 232-2850.

Sincerely,

Enclosure: As stated

Page 2

"CYBERSECURITY: DOD NEEDS TO TAKE DECISIVE ACTIONS TO IMPROVE CYDER HYGIENE"
DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATION

RECOMMENDATION 1:

The GAO recommends that the Secretary of Defense should ensure that the DOD CIO takes appropriate steps to ensure that the DC31 tasks are implemented. (Recommendation 1)

DoD RESPONSE: DoD partially concurs with Recommendation 1. DoD concurs that Task 2 and 6 should continue to be implemented. They are the only two tasks still being actively pursued because the remaining tasks were either implemented or have been overcome by events. Regarding Task 2, the re-issuance of DoD Directive 8140.01 is in the final stages of formal staffing and is expected to be released by October 2020, and will be followed by the later release of both DoD Instruction 8140.AB (new) and DoD Manual 8140. 01 (new - replaces/cancels DoDM 8570.01). Each one of these issuances are at different stages of development and coordination. The manual, which specifically addresses the cyber workforce education and training requirements, will be last to be published and is expected to take approximately 14 - 18 months to complete. Regarding Task 6, U.S. Cyber Command has indicated it is in the process of developing a resourcing plan to support scheduled inspections and no-notice spot checks.

RECOMMENDATION 2:

The GAO recommends that the Secretary of Defense should ensure that DOD components develop plans with scheduled completion dates to implement the four remaining Cyber Discipline Implementation Plan (CDIP) tasks overseen by DOD CIO. (Recommendation 2)

DoD RESPONSE: DoD partially concurs with Recommendation 2. The unclassified report does not specifically identify the four tasks. We will reserve our detailed response for the classified version of the report.

RECOMMENDATION 3:

The GAO recommends that the Secretary of Defense should ensure the Deputy Secretary of Defense identifies a DOD component to oversee the implementation of the seven CDIP tasks and report on progress implementing them. (Recommendation 3)

DoD RESPONSE: DoD non-concurs with Recommendation 3. The cyber landscape is constantly evolving with changes in technology, threats, and vulnerabilities. This requires DoD to reassess its cybersecurity priorities. Since the CDIP's approval in 2015,…

Page 3

… the Department has issued new or updated versions of the National Defense Strategy, DoD Cyber Strategy, Digital Modernization Strategy, DoD Cloud Strategy, Artificial Intelligence Strategy, and is on the cusp of issuing a DoD Cybersecurity Risk Reduction Strategy. Further, the Deputy Secretary of Defense (DSD) directed

DoD develop a classified Top 10 list of cybersecurity critical risk areas, which is subject to periodic review and update. The classified Top 10 Scorecard provides the DSD with a quarterly assessment of the Department's cybersecurity risk reduction progress in these areas. To require that all of this new strategic direction and prioritization be overridden to monitor compliance with lower risk areas that the DoD identified almost five years ago will frustrate the Department's efforts to keep pace with the changing tactics, techniques, and procedures of our adversaries and the evolving changes in technology.

RECOMMENDATION 4:

The GAO recommends that the Secretary of Defense should ensure that DOD components accurately monitor and report information on the extent that users have completed the Cyber Awareness Challenge training as well as the number who have access to the network revoked due to not completing the training. (Recommendation 4)

DoD RESPONSE: DoD partially concurs with Recommendation 4. DoD concurs that it should ensure DoD components accurately report the number of users completing the required training. However, DoD non-concurs with the recommendation to report the number of users who have had network access temporarily revoked for non-compliance with the annual training requirement. The latter metric would not be meaningful but would be extremely burdensome to collect since network revocations can be for a variety of reasons and cross multiple networks and domains.

Contrary to the report's findings, the Navy indicates that it did provide GAO with the number of users completing the cyber awareness training and the total number of users, from which the number of users not completing the training could be computed.

RECOMMENDATION 5:

The GAO recommends that the Secretary of Defense should ensure that the DOD CIO ensures that all DOD components, including DARPA, require their users to take the Cyber Awareness Challenge training developed by DISA. (Recommendation 5)

DoD RESPONSE: Concur. DoD 8510.01-M currently requires the DISA- developed course be used to meet both the initial and annual awareness training mandated training.

RECOMMENDATION 6:

The GAO recommends that the Secretary of Defense should direct a component to monitor the extent to which practices to protect the department's network from key cyberattack techniques are implemented. (Recommendation 6)

Page 4

RECOMMENDATION 7:

The GAO recommends that the Secretary of Defense should ensure that the DOD CIO assesses the extent to which senior leaders' have complete information to make risk based decisions-and revise the recurring reports (or develop a new report) accordingly. Such information could include DOD's progress on implementing I) cyber hygiene initiatives and (2) cyber hygiene practices to protect DOD networks from key cyberattack. (Recommendation 7)

DoD RESPONSE: DoD partially concurs with Recommendation 7. DoD concurs that it will revise the recurring reports by merging the Cyber Hygiene and Top 10 Scorecards to further assist senior leader decision-making by correlating the data in both scorecards. DoD non-concurs that it is possible to have "complete information to make risk-based decisions." Risk is a function of multiple variables and these variables are continually evolving. Timely, relevant, and correlated information is the best that can be expected.

Appendix IV: GAO Contacts and Staff Acknowledgments

GAO Contacts

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

Nick Marinos at (202) 512-9342 or marinosn@gao.gov

Staff Acknowledgments

In addition to the individuals named above, Tommy Baril (Assistant Director), Kaelin Kuhn (Assistant Director), James P. Klein (Analyst-in-Charge), Tracy Barnes, Amy Bush, Peter Casey, Amie Lesser, Carlo Mozo, Richard Powelson, Michael Silver, Andrew Stavisky, and Walter Vance made significant contributions to this report. Kiana Beshir, Chris Businsky, Shaun Byrnes, and Richard Sayoc also contributed to the report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

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

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@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