Report No. DODIG-2020-089

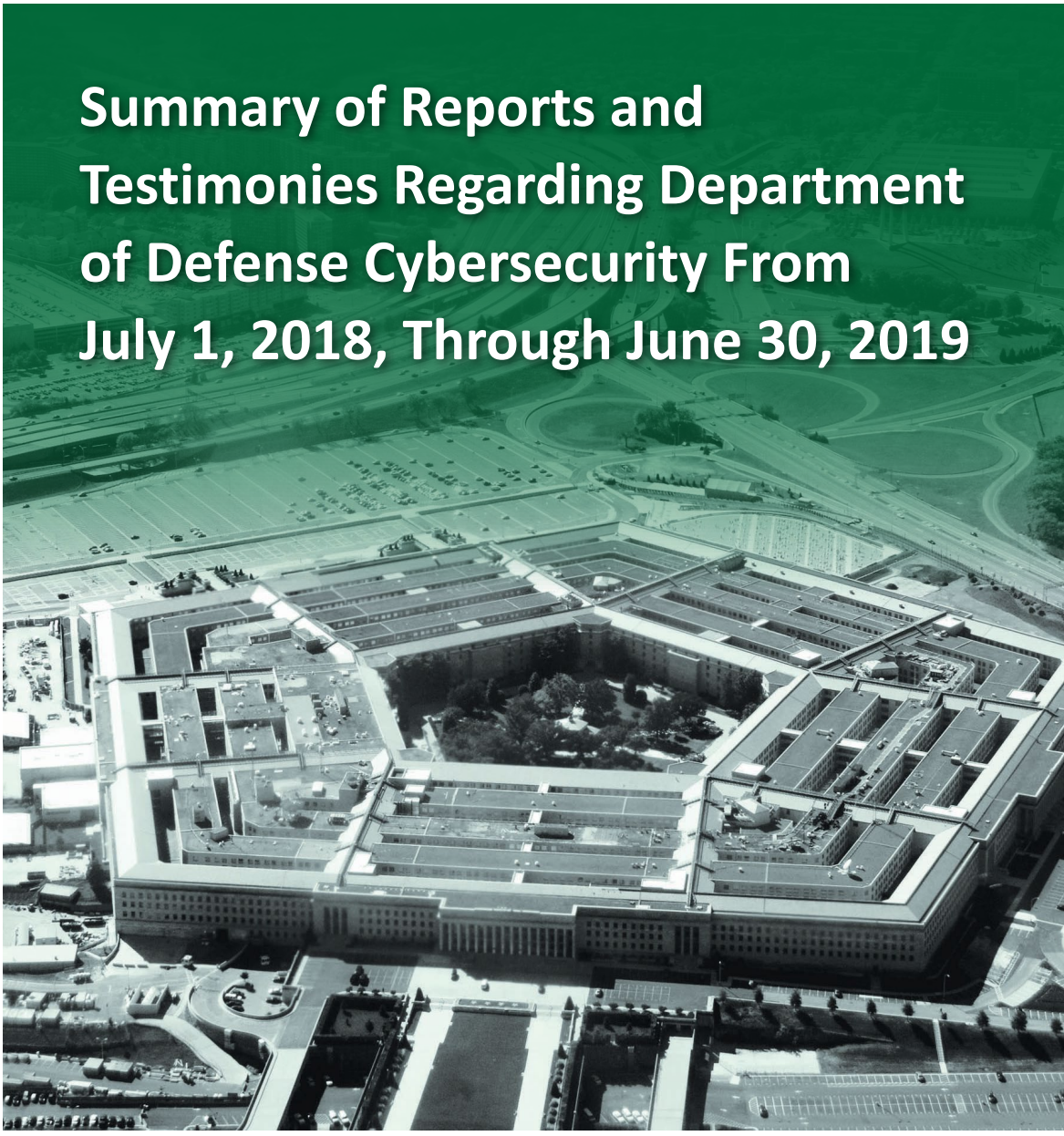
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

JUNE 11, 2020

Summary of Reports and Testimonies Regarding Department of Defense Cybersecurity From July 1, 2018, Through June 30, 2019



INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~The document contains information that may be exempt from mandatory disclosure under the Freedom of Information Act.~~

~~FOR OFFICIAL USE ONLY~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Summary of Reports and Testimonies Regarding Department of Defense Cybersecurity From July 1, 2018, Through June 30, 2019

June 11, 2020

Objective

The objective of this summary report was to: (1) summarize unclassified and classified reports issued and testimony provided to Congress regarding DoD cybersecurity by the DoD Office of Inspector General, the Government Accountability Office, and the other DoD oversight organizations between July 1, 2018, and June 30, 2019; (2) identify cybersecurity risk areas based on the summarized reports and testimonies, and (3) identify the open DoD cybersecurity-related recommendations.

We issue this summary report annually to identify cybersecurity risk areas, based on the National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018, (NIST Cybersecurity Framework), for DoD management to review and consider when implementing changes to improve cybersecurity.

Background

On February 12, 2013, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," which requires NIST to develop a voluntary cybersecurity framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

Background (Cont'd)

On May 11, 2017, the President issued Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which requires Federal agencies use the NIST Cybersecurity Framework to manage their cybersecurity risks. NIST originally released the NIST Cybersecurity Framework on February 12, 2014, and revised it on April 16, 2018. The NIST Cybersecurity Framework has five functions—Identify, Protect, Detect, Respond, and Recover—representing high-level cybersecurity activities that provide a strategic view of the risk management life cycle for identifying, assessing, and responding to risk. For example, the cybersecurity activities for the Identify function include "managing cybersecurity risk to systems, people, assets, data, and capabilities." In addition, the five NIST Cybersecurity Framework functions include 23 associated categories that provide desired cybersecurity outcomes such as "Asset Management" or the "Detection Process." Each of the 23 categories has up to 12 subcategories that further divide the categories into specific outcomes of technical or management activities such as "data at rest is protected" or "notifications from detection systems are investigated."

The DoD has also issued guidance that provides an integrated enterprise-wide decision structure for managing cybersecurity risk. This risk management process is mandatory for managing all the DoD information technologies and is consistent with the principles established by NIST.

Summary

We determined that the DoD Components implemented corrective actions necessary to close 200 of the 530 cybersecurity-related recommendations from issued reports included in this summary report and our prior summary reports. Those corrective actions are intended to mitigate or remediate risks and weaknesses to the DoD systems and networks. However, as of September 30, 2019, the DoD had 330 cybersecurity-related recommendations that remained open, dating back to 2011.

Results in Brief

Summary of Reports and Testimonies Regarding Department of Defense Cybersecurity From July 1, 2018, Through June 30, 2019

Summary (Cont'd)

This year's report summarizes the results of the 46 DoD cybersecurity-related reports issued—33 unclassified and 13 classified—and the content of three testimonies made by the DoD Office Of Inspector General, Government Accountability Office, and the other DoD oversight organizations from July 1, 2018, through June 30, 2019.

Although we include the number of classified reports issued in our discussion of the NIST Cybersecurity Framework functions and categories in this summary, we did not issue classified appendixes summarizing the specific findings and results of those reports due to impact of the coronavirus disease–2019 on classified processing requirements.

We also determined that despite numerous improvements made by the DoD over the past year, recently issued cybersecurity reports demonstrate that the it continues to face significant challenges in managing cybersecurity risks to its systems and networks. For example, the DoD has made improvements related to the NIST Cybersecurity Framework categories of Governance (Identify function), Identity Management and Access Controls (Protect function), and Awareness and Training (Protect function) by issuing new or revised cybersecurity policies and procedures. However, significant risks remain in managing the DoD's cybersecurity activities related to most of the NIST Cybersecurity Framework categories (18 of the 23). The majority of the identified risks and weaknesses relate to the categories of Governance (Identify function), Asset Management (Identify function), Risk Assessment (Identify function), Information Protection Processes and Procedures (Protect function), Awareness and Training (Protect function), and Identity Management and Access Control (Protect function).

These risks generally occurred because the DoD either did not establish policies and procedures to implement minimum standards or they did not effectively implement the necessary controls in accordance with DoD and Federal guidance. For example, the DoD did not

- establish policies and procedures to implement the minimum insider threat standards or requirements related to the Cybersecurity Information Sharing Act of 2014;
- provide oversight of its cyber workforce to ensure consistent implementation of training standards or the proper implementation of system security controls;
- follow established procedures to mitigate or remediate DoD weapon system vulnerabilities or ensure that data were properly removed from removable electronic media such as thumb drives; or
- implement a process to identify the DoD cyber workforce vacancies or rationalize software applications.[1]

Although we are not making new recommendations to the DoD management in this summary report, it is vital to the DoD's overall cybersecurity posture that management implement in a timely manner comprehensive corrective actions that addresses the open cybersecurity-related recommendations. DoD adversaries such as Russia, China, Iran, and North Korea; terrorist groups; hacktivists; and other independent malicious actors can exploit these

[1] Rationalization is the process of identifying all software applications owned and in use on the enterprise network; determining whether existing software applications are needed, duplicative, or obsolete; taking appropriate action to keep or eliminate a software application; and determining whether a software application already exists within the enterprise before purchasing an application.

Results in Brief

Summary of Reports and Testimonies Regarding Department of Defense Cybersecurity From July 1, 2018, Through June 30, 2019

Summary (Cont'd)

cybersecurity vulnerabilities to gain unauthorized access to systems and networks and use sensitive and classified information to collect intelligence, target the DoD critical infrastructures, manipulate information, and conduct cyber attacks. Therefore, the DoD must ensure that it periodically identifies and manages its cybersecurity-related risks appropriately, has a skilled workforce capable of conducting necessary cyber missions, and implements processes to monitor and protect the DoD Information Network.

Additionally, during the FY 2018 and FY 2019 DoD financial statement audits, the DoD Office of Inspector General and independent public accounting firms' auditors identified the need for the DoD to develop and implement more effective internal controls for 247 information technology systems that process transactions for financial reporting, including controls to manage user accounts, monitor user activities, and secure the systems that process financial transactions that are reported on financial statements. A significant function of financial statement audits is reviewing information technology and cyber security. In FY 2019, auditors reported that the DoD and 13 of its Components had a material weakness related to their financial management systems, as well as their information technology environments.

As of December 31, 2019, the DoD had more than 1,500 open information technology notices of findings and recommendations (NFR) as a result of the FY 2018 and FY 2019 financial statement audits.[2] We determined that some of these NFRs identified weaknesses relating to the NIST Cybersecurity Framework. The majority of the NFRs reviewed related directly to the concepts covered in the Protect function of the NIST Cybersecurity Framework, including the categories of Identity Management and Access Control, Information Protection Processes and Procedures, Protective Technology, and Data Security. For example, the auditors identified that the DoD did not:

- appropriately restrict access rights and responsibilities according to segregation of duties policy (Identity Management and Access Control category);
- terminate user access in a timely manner when users left the organization (Identity Management and Access Control category);
- implement controls to identify unintentional or unauthorized changes made to applications, databases, or data (Information Protection Processes and Procedures category); or
- perform reconciliations between systems to verify the completeness and accuracy of data being transferred (Data Security).

Ineffective system controls can result in significant risk to the DoD assets. For example, payments and collections could be lost, stolen, or duplicated as a result of weak information technology controls. Implementing the recommended actions included in these NFRs will better enable the DoD to improve its overall reliance on the accuracy and completeness of financial-data. In addition, improving internal controls for information technology systems that process financial transactions can improve not only financial management but also the overall cybersecurity of the DOD Information Network and better assist in protecting against and rapidly responding to cyber threats across its various networks and systems.

[2] NFR's are used communicate to management in a timely manner any identified weaknesses and inefficiencies in financial processes, the impact of these weaknesses and inefficiencies, the reason the weaknesses and inefficiencies exist, and recommendations to management on how to correct the weaknesses and inefficiencies.

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

June 11, 2020

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Summary of Reports and Testimonies Regarding Department of Defense Cybersecurity From July 1, 2018, Through June 30, 2019 (Report No. DODIG-2020-089)

We are providing this report for your information and use. We conducted this summary work in accordance with generally accepted government auditing standards except for the standards of planning and evidence because the report summarizes previously released reports.

The report contains no recommendations; however, it does identify previously issued audit reports that contain recommendations issued during the reporting period. We did not issue a draft report and no written response is required.

We appreciate the cooperation and assistance received during this audit. Please direct questions to me at [redacted]

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Distribution:

DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
COMPTROLLER GENERAL, GOVERNMENT ACCOUNTABILITY OFFICE
COMMANDER, U.S. CYBER COMMAND
DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE NAVY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

Contents

Introduction

Objective

The objective of this summary report was to: (1) summarize unclassified and classified reports issued and testimonies provided to Congress regarding DoD cybersecurity by the DoD Office of Inspector General (OIG), the Government Accountability Office (GAO), and the other DoD oversight organizations between July 1, 2018, and June 30, 2019; (2) identify cybersecurity risk areas based on the summarized reports and testimonies, and (3) identify the open DoD cybersecurity-related recommendations.[3]

We issue this summary report annually to identify cybersecurity risk areas based on the National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018 (NIST Cybersecurity Framework) for DoD management to review and consider when implementing changes to improve cybersecurity. See Appendix A for a discussion of the scope and methodology and a list of previously issued cybersecurity summary reports. See Appendix B for a list of the unclassified and classified reports and testimonies summarized in this report.

[3] Open recommendations can be either resolved or unresolved. Resolved recommendations are those that the DoD management has agreed to implement, but for which management has not yet completed agreed-upon actions. Unresolved recommendations are those that the DoD management has not agreed to implement or proposed actions that will not address the intent of the recommendation.

Background

The DoD depends on cyberspace to support its business and military operations and, therefore, must be able to defend its own networks, systems, and information from malicious cyber activity and be prepared to defend, when directed, those networks and systems operated by non-DoD Defense Critical Infrastructure and Defense Industrial Base entities.[4] The DoD needs to continuously assess and adapt its cyberspace capabilities to defend the DoD Information Network (DODIN) and the systems and networks of the DoD's partners and allies.

The DODIN is a global set of data, capabilities, and processes interconnected for collecting, processing, storing, disseminating, and managing real time information for the warfighter, policy makers, and support personnel. The DODIN comprises approximately 10,000 operational systems, thousands of data centers, tens of thousands of servers, and millions of computers and information technology devices. Much of the DODIN is old, making it difficult to secure the systems and networks against cybersecurity threats.

Additionally, the scope and pace of malicious cyber activity continues to increase from foreign countries, such as Russia, China, Iran, and North Korea. In 2019, the GAO stated in a report related to threats facing the U.S., that Government agencies identified Chinese global expansion as a threat, which may include cyber and electronic warfare.[5] In addition, the Director of National Intelligence stated in January 2019 testimony "Our adversaries and strategic competitors will increasingly use cyber capabilities—including cyber espionage, attack, and influence—to seek political, economic, and military advantage over the United States and its allies and partners."[6]

DoD Risk Management Framework

Cybersecurity risk management comprises the full range of activities undertaken to protect information and information technology from cyber threats, such as unauthorized system access and loss of data. DoD Instruction 8500.01 establishes the DoD Cybersecurity Program to protect and defend DoD information and information technology.[7] According to the Instruction, all DoD information

[4] According to the Summary of the 2018 DoD Cyber Strategy, released on September 18, 2018, Defense Critical Infrastructure refers to the composite of the DoD and non-DoD assets essential to project, support, and sustain military forces and operations worldwide and Defense Industrial Base refers to the DoD, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements.

[5] GAO Report No. GAO-19-204SP, "National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies," December 13, 2018.

[6] Statement to the U.S. Senate Select Committee on Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," January 29, 2019.

[7] DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (Incorporating Change 1, Effective October 7, 2019).

technology must be assigned to, and governed by, a DoD Component cybersecurity program that manages risk commensurate with the importance of supported missions and the value of potentially affected information and assets.
DoD Instruction 8510.01 provides an integrated enterprise-wide risk management structure, known as the DoD Risk Management Framework (RMF).[8] This risk management process is mandatory for managing all DoD information technologies and is consistent with the principles established in the NIST Cybersecurity Framework and the Risk Management Framework (NIST Special Publication 800-37).[9]

NIST Cybersecurity Framework

In February 2013, the President issued Executive Order 13636 , 3 CFR, Sec 7(a) directing NIST to develop a voluntary cybersecurity framework that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to help the owners and operators of critical infrastructure identify, assess, and manage cybersecurity risk.[10] The Cybersecurity Enhancement Act of 2014 further codified requirements for NIST to develop an approach to help identify, assess, and manage cybersecurity risk for critical infrastructure.[11]

To improve accountability for managing enterprise cybersecurity risks, the President issued Executive Order 13800 in May 2017 requiring Federal agencies to use the NIST Cybersecurity Framework to manage their cybersecurity risk.[12] The Office of Management and Budget also issued guidance in May 2017 to support Federal agencies in implementing Executive Order 13800 requirements.[13]

The NIST Cybersecurity Framework establishes a risk-based approach to managing cybersecurity risk by providing an organization with a common set of cybersecurity activities, desired outcomes, and criteria.[14] All of these things allow the organization to communicate using a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. The NIST Cybersecurity Framework can also be used to help identify and prioritize actions for reducing cybersecurity risk and to align policy, business, and technological approaches to managing that risk.

---

8 DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology," March 12, 2014 (Incorporating Change 2, July 28, 2017).

9 NIST "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018. NIST Special Publication 800-37, Revision 2, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," December 2018.

10 Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013.

11 Public Law 113-274, "Cybersecurity Enhancement Act of 2014," December 18, 2014.

12 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017.

13 Office of Management and Budget Memorandum M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 19, 2017.

14 For this report, we consider criteria as any informative references as well as industry standards, guidelines, and practices provided by the NIST Cybersecurity Framework.

Risk Management

According to the NIST Cybersecurity Framework, risk management is the ongoing process of identifying, assessing, and responding to risk. Organizations should understand the likelihood that an event, such as unauthorized access resulting in stolen or destroyed information, will occur and the potential resulting impacts to manage that risk. Organizations should then determine the acceptable level of risk for achieving their organizational objectives and express this level as their risk tolerance. After establishing the risk tolerance, organizations can then prioritize cybersecurity activities, such as software updates and access controls, enabling organizations to make informed decisions about cybersecurity resources.

An organization can use the NIST Cybersecurity Framework as a key part of its process for identifying, assessing, and managing cybersecurity risk. The NIST Cybersecurity Framework is not designed to replace existing cybersecurity processes; instead, an organization can use its own existing process and apply the NIST Cybersecurity Framework to determine whether the organization has any gaps in cybersecurity and develop a plan for improvement. Using the NIST Cybersecurity Framework as a cybersecurity risk management tool enables an organization to determine activities that are most important to critical service delivery and prioritize resources to maximize the impact of those activities.

NIST Cybersecurity Framework Functions and Categories

The NIST Cybersecurity Framework is a common set of activities for managing cybersecurity risk and has five functions—Identify, Protect, Detect, Respond, and Recover—representing high-level cybersecurity activities that provide a strategic view of the risk management lifecycle for identifying, assessing, and responding to risk. For example, the cybersecurity activities for the Identify function include "managing cybersecurity risk to systems, people, assets, data, and capabilities," while the activities for the Recover function include the "plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident."

Additionally, the five NIST Cybersecurity Framework functions include 23 associated categories that provide desired cybersecurity outcomes such as "Asset Management" or the "Detection Process." Each of the 23 categories has up to 12 subcategories that further divide the categories into specific outcomes of technical or management activities such as "data-at-rest is protected" or

"notifications from detection systems are investigated." See Appendix C for the NIST Cybersecurity Framework's five functions and 23 categories and the desired cybersecurity outcomes of each function and category. Table 1 lists the five functions and the 23 corresponding categories.

Table 1. NIST Cybersecurity Framework Categories by Function

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
	Supply Chain Risk Management
Protect	Identity Management and Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

Source: NIST Cybersecurity Framework.

Summary

Cybersecurity Risks Remain a Significant Challenge for the DoD

We determined that the DoD Components implemented corrective actions necessary to close 200 of the 530 cybersecurity-related recommendations from issued reports included in this summary report and our prior summary reports.[15] Those corrective actions are intended to mitigate or remediate risks and weaknesses to DoD systems and networks. However, as of September 30, 2019, the DoD had 330 cybersecurity-related recommendations that remained open, dating back to 2011.[16]

This year's report summarizes the results of the 46 DoD cybersecurity-related reports issued—33 unclassified and 13 classified—and the content of three testimonies provided to Congress by the DoD OIG, GAO, and the other DoD oversight organizations from July 1, 2018, through June 30, 2019.[17] Although we include the number of classified reports issued in our discussion of the NIST Cybersecurity Framework and categories, we did not issue classified appendixes summarizing the specific findings and results of those reports due to impact of the coronavirus disease–2019 on classified processing requirements.

We also determined that despite numerous improvements made by the DoD over the past year, recently issued cybersecurity reports demonstrate that the DoD continues to face significant challenges in managing cybersecurity risks to its systems and networks. For example, the DoD made improvements relating to the NIST Cybersecurity Framework categories of Governance (Identify function), Identity Management and Access Controls (Protect function), and Awareness and Training (Protect function) by issuing new or revised cybersecurity policies and procedures. However, significant risks remain in managing the DoD's cybersecurity activities related to most of the NIST Cybersecurity Framework categories (18 of the 23).

The majority of the identified risks and weaknesses relate to the categories of Governance (Identify function), Asset Management (Identify function), Risk Assessment (Identify function), Information Protection Processes and Procedures (Protect function), Awareness and Training (Protect function), and the Identity

[15] See Appendix A for a listing of prior cybersecurity summary reports over the last five years.

[16] See Appendix E for a matrix of open recommendations organized by NIST Cybersecurity Framework function.

[17] See Appendix B for a list of all unclassified and classified reports and testimonies regarding the DoD cybersecurity issues during this period.

Management and Access Control (Protect function). See Appendix D for a list of reports and testimonies identifying cybersecurity risks by the NIST Cybersecurity Framework category.

These risks generally occurred because the DoD either did not establish policies and procedures to implement minimum standards or it did not effectively implement the necessary controls in accordance with DoD and Federal guidance. For example, the DoD did not:

- establish policies and procedures to implement the minimum insider threat standards or requirements related to the Cybersecurity Information Sharing Act of 2014 (CISA);[18]
- provide oversight of its cyber workforce to ensure consistent implementation of training standards or the proper implementation of system security controls;
- follow established procedures to mitigate or remediate DoD weapon system vulnerabilities or ensure that data were properly cleared from removable electronic media such as thumb drives (removable media sanitization); or
- implement a process to identify DoD cyber workforce vacancies or rationalize software applications.[19]

Although we are not making new recommendations to DoD management in this summary report, it is vital to the DoD's overall cybersecurity posture that management implement in a timely manner comprehensive corrective actions identified in the reports we reviewed that address the open cybersecurity-related recommendations. DoD adversaries such as Russia, China, Iran, and North Korea; terrorist groups; hacktivists; and other independent malicious actors can exploit these cybersecurity vulnerabilities to gain unauthorized access to systems and networks and use sensitive and classified information to collect intelligence, target the DoD critical infrastructures, manipulate information, and conduct cyber attacks. Therefore, the DoD must ensure that it periodically identifies and manages its cybersecurity-related risks appropriately, has a skilled workforce capable of conducting necessary cyber missions, and implements processes to monitor and protect the DODIN.

[18] Public Law 114-113, "Division N—Cybersecurity Act of 2015, Title I—Cybersecurity Information Sharing," December 18, 2015.

[19] Rationalization is the process of identifying all software applications owned and in use on the enterprise network; determining whether existing software applications are needed, duplicative, or obsolete; taking appropriate action to keep or eliminate a software application; and determining whether a software application already exists within the enterprise before purchasing an application.

Additionally, during the FY 2018 and the FY 2019 DoD financial statement audits, the DoD OIG and independent public accounting firms' auditors identified the need for the DoD to develop and implement more effective internal controls for 247 information technology systems that process transactions for financial reporting, including controls to manage user accounts, monitor user activities, and secure the systems that process financial transactions that are reported on financial statements. A significant function of financial statement audits is reviewing information technology and cyber security. In FY 2019, auditors reported that the DoD and 13 of its components had a material weakness related to financial management systems, as well as the their information technology environments. As of December 31, 2019, the DoD had more than 1,500 open information technology notices of findings and recommendations (NFR) as a result of the FY 2018 and FY 2019 financial statement audits.[20] We determined that some of these NFRs identified weaknesses relating to the NIST Cybersecurity Framework.

In January 2020, the DoD OIG summarized the large amounts of control deficiencies affecting the financial systems used by the DoD Components.[21] These deficiencies represent significant cybersecurity risks affecting the integrity and accuracy of the data stored and processed by the DoD. The majority of the NFRs reviewed related directly to the concepts covered in the Protect function of the NIST Cybersecurity Framework, including the categories of Identity Management and Access Control, Information Protection Processes and Procedures, Protective Technology, and Data Security. For example, the DoD did not:

- ~~(FOUO)~~ [redacted][22]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

[20] NFRs are used communicate to management in a timely manner any identified weaknesses and inefficiencies in financial processes, the impact of these weaknesses and inefficiencies, the reason the weaknesses and inefficiencies exist, and recommendations to management on how to correct the weaknesses and inefficiencies.

[21] DoD OIG Report, "Understanding the results of the Audit of the DoD FY 2019 Financial Statements," January 28, 2020.

[22] ~~(FOUO)~~ [redacted]

[23] ~~(FOUO)~~ [redacted]

[24] ~~(FOUO)~~ [redacted]

- ~~(FOUO)~~ [redacted]

Ineffective system controls can result in significant risk to the DoD assets. For example, payments and collections could be lost, stolen, or duplicated as a result of weak information technology controls. Implementing the recommended actions included in the NFRs will better enable the DoD to improve its overall reliance on the accuracy and completeness of financial data. In addition, improving internal controls for information technology systems that process financial transactions can improve not only financial management but also the overall cybersecurity of the DODIN and better assist in protecting against and rapidly responding to cyber threats across its various networks and systems.

Actions Taken to Improve the DODIN's Security Posture

The DoD Components took corrective actions to close the 200 DoD cybersecurity-related recommendations that addressed a variety of cybersecurity risks, such as controlling asset inventories and system access, and providing cybersecurity-related training. The closed cybersecurity-related recommendations were comprised of 101 recommendations identified in the reports summarized in the FY 2018 cybersecurity summary report, dating back to FY 2008, and 99 recommendations made in the reports summarized in this summary report. For example:

- To address recommendations made in a FY 2017 report relating to data deficiencies contained in the DoD Information Technology Portfolio Repository, the DoD Chief Information Officer (CIO) implemented a monthly process to notify the DoD Components of data repository errors and hold Component CIOs accountable for the accuracy and completeness of the data. Consequently, the DoD Components have maintained a higher level of data quality and data completeness.
- ~~(FOUO)~~ [redacted]

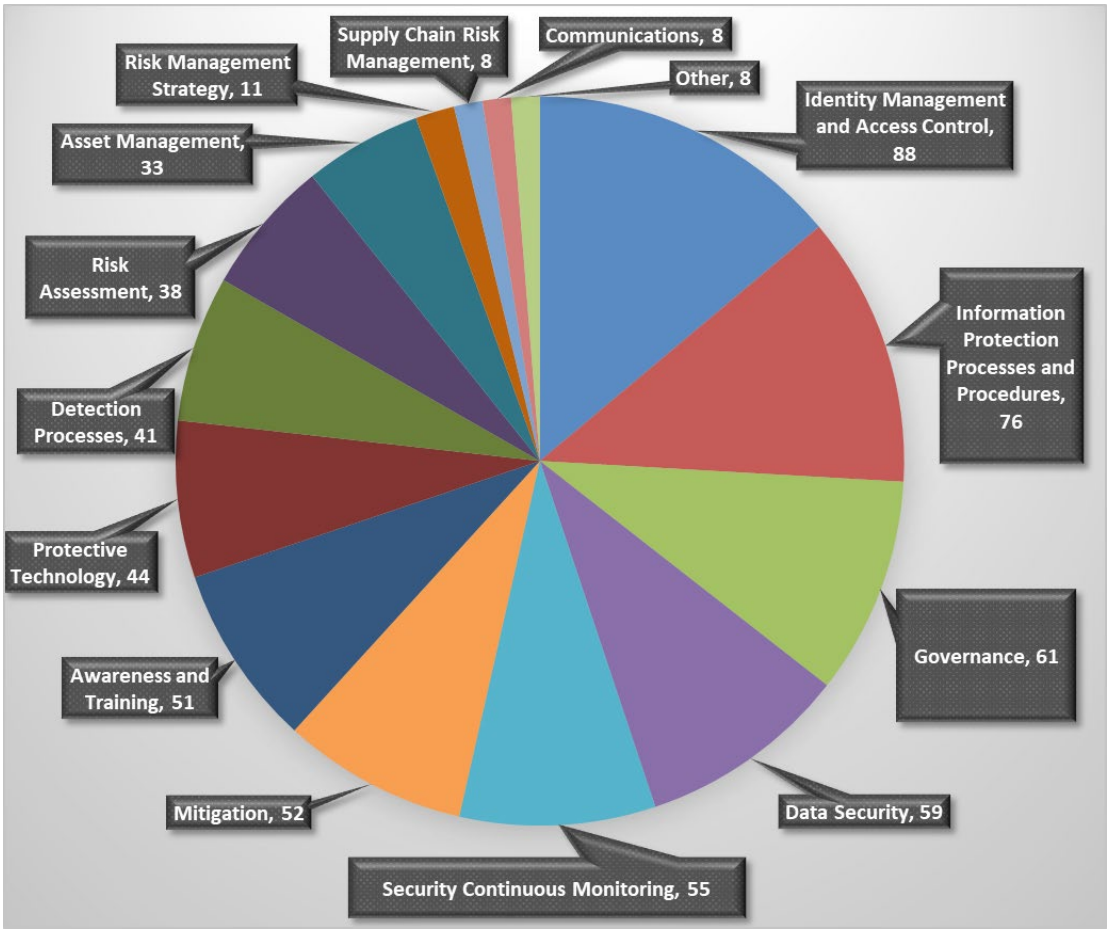
[25] ~~(FOUO)~~ [redacted]

- To address recommendations made in a FY 2017 report relating to security management, access, configuration management, and contingency planning controls, officials in the Business Enterprise Information Services Office developed, revised, disseminated, and implemented policies and procedures and trained cybersecurity personnel on the specific requirements for application level general controls.[26] These actions helped improve the design and operating effectiveness of several key application level general controls including security management, access controls, configuration management, and contingency management.
- ~~(FOUO)~~ [redacted]

As a result of corrective actions taken, the DoD improved its overall security of the DODIN and the DoD Component specific systems and programs in areas such as asset management, identity and access controls, cybersecurity workforce management, and training. However, recently issued cybersecurity reports identify that the DoD continues to face significant challenges in managing cybersecurity risk to its systems, networks, and devices. As of September 30, 2019, the DoD had 330 open cybersecurity-related recommendations—297 unclassified and 33 classified—made in reports issued as far back as 2011. Figure 1 shows the number of open DoD cybersecurity-related recommendations by NIST Cybersecurity Framework category.

[26] According to GAO Report No. GAO-09-232G, "Federal Information System Controls Audit Manual (FISCAM), February 2, 2009, application level general controls consist of general controls operating at the business process application level, including those related to security management, access controls, configuration management, segregation of duties, and contingency planning.

Figure 1. Number of Open DoD Cybersecurity-Related Recommendations by NIST Cybersecurity Framework Category



Note: The "other" category is comprised of 9 of the 23 NIST Cybersecurity Framework categories.
Source: The DoD OIG.

Although we are not making new recommendations to the DoD management in this summary report, it is vital to the DoD's overall cybersecurity posture that management timely implement comprehensive corrective actions that address the open recommendations. As cyber attacks are becoming more sophisticated; malicious tools more prevalent; and information technology systems, networks, and devices more interconnected, the DoD must ensure that it not only takes corrective actions on open recommendations, but also implement effective risk management practices to reduce cybersecurity risks affecting the DODIN and all business and military operations.

Challenges Remain in Managing DoD Cybersecurity Risks

Between July 1, 2018, through June 30, 2019, the DoD OIG, GAO, and the other the DoD oversight organizations issued 46 reports—33 unclassified and 13 classified—and provided testimony made at three Congressional hearings, identifying significant challenges that the DoD faces in managing cybersecurity risks. Overall, this year's summary highlights that the DoD needs to continue focusing corrective actions on cybersecurity weaknesses affecting the NIST Cybersecurity Framework categories of Governance (Identify function), Asset Management (Identify function), Risk Assessment (Identify function), Information Protection Processes and Procedures (Protect function), Awareness and Training (Protect function), and the Identity Management and Access Control (Protect function).

~~(FOUO)~~ In this year's sumemary report, we determined that the category with the most identified risks or weaknesses was the Governance category, under the Identify function. In general, 29 of the 46 issued reports stated that the DoD officials did not have controls in place or take the steps needed to ensure that the DoD Components fully implemented established policies and procedures. For example, in one report, [redacted]

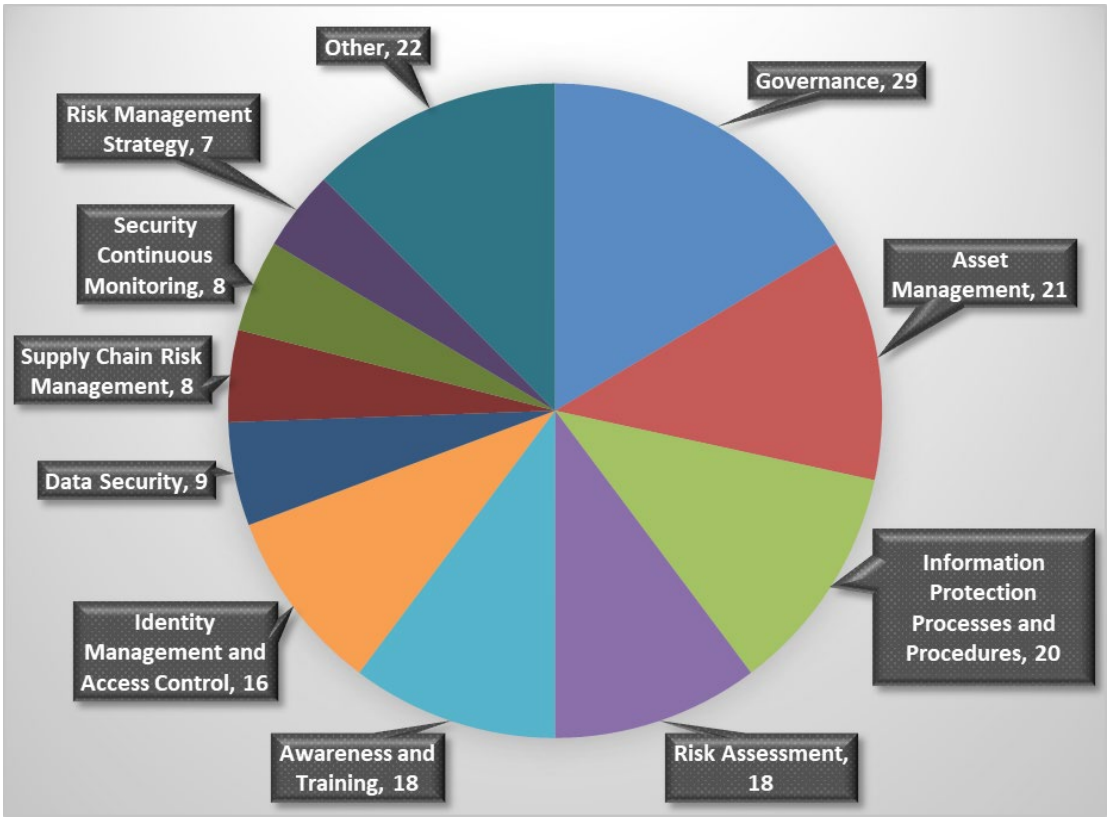
We also determined that other significant cybersecurity risks identified in the 46 reports issued and 3 testimonies provided to Congress relate to vendor risk management (Supply Chain Risk Management category), asset vulnerability identification (Risk Assessment category), access controls (Identity Management and Access Controls category), risk decisions documentation (Risk Management Strategy category), and data protection (Data Security category). Without adequate controls in those areas, the DoD cannot ensure that:

- contractors and third-party partners implement necessary cybersecurity measures or controls,
- cybersecurity vulnerabilities for information systems, networks, and devices are identified and managed, or

- data that are stored and processed by DoD systems, networks, and devices are protected from unauthorized access.[27]

The reports also identified risks in key subcategories such as remediating identified vulnerabilities and sharing cyber threat information, highlighting the risks to the DoD information and the barriers to sharing cyber threat indicators and defensive measures. Figure 2 shows the reports and testimonies identifying risks by NIST Cybersecurity Framework category.

Figure 2. Number of Reports and Testimonies with Risks Identified by NIST Cybersecurity Framework Category



Note: The "other" category is comprised of 13 of the 23 NIST Cybersecurity Framework categories.
Source: The DoD OIG.

[27] Access controls, such as managing physical and remote access, are subcategories of the Identity Management and Access Control category. Identifying and documenting asset vulnerabilities is a subcategory of the Risk Assessment category.

Risks by NIST Cybersecurity Framework

Between July 1, 2018, through June 30, 2019, the DoD OIG, GAO, and the other the DoD oversight organizations issued 46 reports—33 unclassified and 13 classified—and three testimonies provided to Congress that identified cybersecurity risks in four of the five NIST Cybersecurity Framework functions—Identify, Protect, Detect, and Respond. Table 2 provides the number of reports, by oversight agency, which identify risks and improvements related to each NIST Cybersecurity Framework function.[28]

Table 2. Number of Reports and Testimonies Identifying Risks by NIST Cybersecurity Framework Function

Function	GAO	DoD OIG	Army Audit Agency	Naval Audit Service	Air Force Audit Agency	Other DoD Agencies	Total
Identify	10*	11	4	5	5	4	39
Protect	5*	11	3	4	5	5	33
Detect	1	5	0	2	0	2	10
Respond	1	6	0	0	1	0	8
Recover	0	0	0	0	0	0	0

Note: Totals do not equal the number of reports and testimonies identified because one report or testimony may cover more than one NIST Cybersecurity Framework function.

*One testimony is included in the quantities above. The remaining two testimonies are not included because they address cybersecurity-related issues already accounted for within a GAO report.

Source: The DoD OIG.

Identify Function

We determined that there were 38 reports issued—30 unclassified and 8 classified—and one testimony provided to Congress that identified risks related to the Identify function, primarily within the Governance, Asset Management, and Risk Assessment categories. The Identify function includes activities that assist an organization in managing cybersecurity risk to systems, people, assets, data, and capabilities. These reports and the testimony identified risks and weaknesses relating to the Identify function—such as the establishment of well-defined cybersecurity roles and responsibilities and the consistent sharing of cybersecurity information—that assists an organization in effectively managing its cybersecurity risks impacting operations, resources, and assets. Table 3 provides the NIST Cybersecurity Framework categories under the Identify function and the desired cybersecurity activities and outcomes.

[28] Appendix D provides a list of reports identifying cybersecurity risks by NIST Cybersecurity Framework function and category.

Table 3. NIST Cybersecurity Framework Categories for the Identify Function

Function	Category	Cybersecurity Outcomes
Identify	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and risk strategy.
	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.

Source: NIST Cybersecurity Framework.

Additionally, some of the reports identified risks in the other three categories under the Identify function—Business Environment, Risk Management Strategy, and Supply Chain Risk Management. Examples of risks identified in reports that are not summarized in the Identify function sections below include:

- The DoD did not provide guidance that clearly defined the roles and responsibilities for user involvement and feedback during software development. As a result, officials who manage software-intensive space program did not obtain the necessary feedback to avoid delivering software that would be operationally unsuitable and required significant rework.

- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

To address the cybersecurity risks in the Identify function, DoD officials need to understand the DoD's business operations, the resources—such as, hardware, devices, data, time, personnel, and software—that support critical functions and the related cybersecurity risks. The DoD also needs to focus and prioritize its efforts to address cybersecurity risk to systems, people, assets, data, and capabilities, consistent with its risk management strategy and business needs.

The following sections provide examples from unclassified reports that identified risks caused by a lack of sufficient oversight in the three main categories under the Identify function—Governance, Asset Management, and Risk Assessment. In each category we provide the number of reports that identified risks, the definition of the category, and an overview of the cybersecurity risks with associated causes and examples. For each example, we provide a summary of the report's findings, causes, effects, and status of the recommendations made along with an example of a recommendation.

Governance Category

We determined that there were 29 issued reports that identified risks relating to the Governance category. The NIST Cybersecurity Framework defines Governance category outcomes as those that allow an organization to inform its management of cybersecurity risk through policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements. The reports identified risks related to such things as cybersecurity workforce requirements and the implementation guidance of the CISA requirements. However, the reports also highlighted proactive actions taken by the DoD to address some of the risks identified.

The 29 reports included recommendations for the DoD to establish or update policies, processes, and procedures used to manage and monitor the DoD's regulatory, legal, and operational requirements, ensuring that requirements such as those prescribed in CISA are met. The following reports identified cybersecurity risks related to the Governance category and the impact of the risks.

GAO Report No. GAO-19-144, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," March 12, 2019

The GAO reviewed 24 Federal agencies, including the DoD, to determine the extent to which these agencies performed cybersecurity workforce planning, as required by the Federal Cybersecurity Workforce Assessment Act of 2015.[29] The GAO determined that most of these agencies assigned work roles to both filled and vacant positions that performed information technology, cybersecurity, or cyber-related functions. However, the GAO determined that the DoD did not meet the requirement to do so. The GAO also determined that the 24 agencies began to identify critical information technology, cybersecurity, or cyber-related staffing needs.

The Federal Cybersecurity Workforce Assessment Act of 2015 requires the Office of Personnel Management and Federal agencies to categorize all information technology, cybersecurity, and cyber-related positions using Office of Personnel Management personnel codes for specific work roles; and identify critical staffing needs.[30] Office of Personnel Management guidance directs agencies to identify filled and vacant positions with information technology, cybersecurity, or cyber-related functions and assign work role codes to those positions using the Federal Cybersecurity Coding Structure.[31] This coding structure designates a unique three-digit code for each work role defined in the National Initiative for Cybersecurity Education framework.[32] According to Office of Personnel Management guidance, agencies can assign up to three work role codes to each position, and should assign the code of "000" only to positions that do not perform information technology, cybersecurity, or cyber-related functions.

---

[29] Public Law 114-113, "Consolidated Appropriations Act, 2016," division N, "Cybersecurity Act of 2015," title III, "Federal Cybersecurity Workforce Assessment Act of 2015," December 18, 2015. The Act requires the Office of Personnel Management and Federal agencies to take several actions related to cybersecurity workforce planning.

[30] Office of Personnel Management, "Federal Cybersecurity Coding Structure," Version 2.0, October 18, 2017.

[31] Office of Personnel Management, Memorandum for Heads of Executive Departments and Agencies, "Guidance for Assigning New Cybersecurity Codes to Positions with Information Technology, Cybersecurity, and Cyber-Related Functions," January 4, 2017.

[32] NIST Special Publication 800-181, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," August 2017. The Framework outlines the cybersecurity coding structure and identifies a unique numeric code for each of the 52 work roles and 33 specialty areas defined in the guidance. Work roles provide a more detailed description of the roles and responsibilities of information technology, cybersecurity, and cybersecurity related job functions than do the category and specialty area components of the framework.

Pertaining to the DoD only, the GAO determined that officials did not do the following:

- assign the associated work role codes to vacant positions by April 2018 because the DoD did not have an enterprise-wide capability to assign codes to vacant positions and had not modified its personnel systems to use the three-digit work role codes for vacant positions due to timing and funding constraints.
- categorize the work roles of many positions within the 2210 occupational series correctly.[33] For instance, the GAO determined that the DoD assigned the "000" code to 5 percent of its positions in the 2210 information technology management occupational series, and that these positions were most likely to perform information technology, cybersecurity, or cyber-related functions. DoD human resources and information technology officials said that they may have assigned the "000" code in error.
- categorize the work roles for many positions consistent with their position descriptions. For example, of the 20 work role, coded positions reviewed within the 2210 occupational series, 5 of the positions' assigned codes were inconsistent with the position description text and 4 were missing position descriptions (not provided). DoD CIO officials stated that this occurred because of the large number of positions that perform information technology, cybersecurity, or cyber related functions for the DoD and the lack of mapping those positions to National Initiative for Cybersecurity Education work roles.

The GAO also determined that the 24 agencies began to identify critical needs, and that the DoD submitted a preliminary report of work role critical needs to the Office of Personnel Management by the August 31, 2018, deadline that included the required work role critical information technology, cybersecurity, and cyber-related staffing needs and the root causes of the critical needs identified. However, the DoD had not submitted a report to the Office of Personnel Management substantiating work roles of critical need because they were not required to do so until April 2019.

The GAO stated that until agencies accurately categorize their positions, their ability to effectively identify critical staffing needs will be impaired. The GAO recommended that the Secretary of Defense complete the identification and coding of vacant positions for those positions that perform information

[33] An occupational series is a grouping of positions with a similar line of work and qualification requirements. For example, the 2210 information technology management occupational series covers positions that manage, supervise, lead, administer, develop, deliver, and support information technology systems and services. This series covers positions for which the paramount requirement is knowledge of information technology principles, concepts, and methods.

technology, cybersecurity, or cyber-related functions, and review the general code assignment for the 2210 occupational series—information technology management occupational positions—assign the appropriate work role codes, and assess the accuracy of position descriptions. The DoD CIO agreed with the recommendations, stating that the DoD's long term plan was to code all positions in the DoD's manpower requirements systems and continue to remediate erroneously coded positions. As of September 30, 2019, these recommendations remained open.

DODIG-2019-016, "DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements," November 8, 2018

The DoD OIG determined that, as a result of the inconsistent implementation of CISA by the DoD Components, the DoD limited its ability to gain a more complete understanding of increasing and persistent cybersecurity threats by leveraging the collective knowledge and capabilities of sharing entities. The DoD can provide its Components, other Federal entities, and non-Federal entities access to cybersecurity information that might not be available to them by sharing cyber threat indicators and defensive measures. Using the shared information, entities can improve their security posture by identifying affected systems, implementing protective measures, and responding to and recovering from incidents. This is critical because cyber attackers continually adapt their tactics, techniques, and procedures to evade detection, circumvent security controls, and exploit new vulnerabilities.

~~(FOUO)~~ The DoD OIG made nine recommendations in this report, including actions for the DoD CIO, in coordination with the Under Secretary of Defense for Policy, to develop and issue the DoD-wide policy for implementing CISA requirements. This DoD-wide policy should also include a requirement for the DoD Components to document barriers to sharing cyber threat indicators and defensive measures, and take appropriate actions to mitigate the identified barriers. [redacted]

As of September 30, 2019, eight of the nine recommendations, including those listed above, remained open.

Naval Audit Service Report No. N2019-0029, "Followup on Information Security Within the U.S. Marine Corps," April 2, 2019

(FOUO) [redacted]

(FOUO) [redacted]

- (FOUO) [redacted]

[34] (FOUO) [redacted]

- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

Governance Category Takeaway

We determined that despite improvements made by the DoD over the past year, there were 29 recently issued cybersecurity-related reports that demonstrate that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Governance category. For example, these reports identified risks specific to the inaccurate cyber workforce identification, incorrect classification of positions, insufficient guidance for implementing CISA requirements, and outdated command cybersecurity guidance. By implementing the recommendations identified in these reports, the DoD will gain an understanding of cybersecurity workforce requirements, strengthen its cybersecurity guidance, and ensure that procedures are in place to communicate cybersecurity risks.

Asset Management Category

We determined that there were 20 issued reports and one testimony provided to Congress that identified risks relating to the Asset Management category. The NIST Cybersecurity Framework defines Asset Management category outcomes as those actions that allow an organization to identify and manage its resources—systems, devices, and personnel—to achieve business purposes. The reports and testimony identified risks related to such things as maintaining software and system inventories, rationalizing software applications, and recruiting cybersecurity personnel.[35]

The 20 reports included recommendations for DoD officials to establish or update policies, processes, or controls to correct the risks associated with asset management. The following reports identified cybersecurity risks related to the Asset Management category and the impact of the risks.

DODIG Report No. DODIG-2019-037, "DoD Management of Software Applications," December 13, 2018

The DoD OIG determined that the Navy, Marine Corps, and Air Force commands or divisions reviewed did not consistently rationalize their software applications. The report identified that, although the Navy commands and Marine Corps divisions had a process in place to prevent duplication when purchasing software applications, the Air Force did not. In addition, the report identified that the U.S. Fleet Forces Command was the only command that had a process in place for eliminating duplicative or obsolete software applications it owned. Furthermore, the report identified that none of the seven commands or divisions that were

[35] Rationalization is the process of identifying all software applications owned and in use on the enterprise network; determining whether existing software applications are needed, duplicative, or obsolete; taking appropriate action to keep or eliminate a software application; and determining whether a software application already exists within the enterprise before purchasing an application.

reviewed maintained accurate software inventories to facilitate the software application rationalization process. Software application rationalization did not consistently occur because the DoD CIO did not implement an enterprise-wide solution for software application rationalization and, instead, limited rationalization to data center consolidation efforts. As a result, the DoD and its Components unnecessarily introduced cybersecurity risks into the DODIN because they were unable to account for their software applications or identify the impact of existing vulnerabilities associated with these software applications.

While the audit was ongoing, the DoD CIO issued a memorandum in July 2018 requiring the DoD to show significant improvement in reporting software inventory by December 2018.[36] The memorandum directed the DoD Components to deploy and use existing software inventory modules to increase the DoD's known software inventory. The DoD CIO stated that the DoD must be able to identify, through automated means, the quantity of installed applications and provide the software inventory to a server or reporting service. Because the DoD CIO took action to improve the DoD software inventory reporting during the audit, the DoD OIG did not make recommendations to the DoD Components to improve the accuracy of their software application inventories.

However, the DoD OIG recommended that the DoD CIO, in coordination with the DoD Chief Management Officer:

- develop an enterprise-wide process for conducting software application rationalization;
- establish guidance requiring the DoD Components to conduct software application rationalization, develop implementing guidance that outlines responsibilities and processes for software application rationalization within their Components; and validate the accuracy of their owned and in-use software application inventory, at least annually; and
- conduct periodic reviews to ensure the DoD Components are regularly validating the accuracy of their inventory of owned and in-use software applications and eliminating duplicate and obsolete software applications.

The DoD CIO and the DoD Chief Management Officer agreed with the recommendations. As of September 30, 2019, all three recommendations remained open.

[36] DoD CIO Memorandum, "National Defense Authorization Act, Fiscal Year 2017, Section 1653 Compliance, Information Security Continuous Monitoring, Implementing Comply-to-Connect Policy, and Limitations on Software Licensing," July 10, 2018.

Air Force Audit Agency Report No. F2019-0002-O10000, "Cybersecurity of Network Component Purchases," January 22, 2019

~~(FOUO)~~ The Air Force Audit Agency (AFAA) determined that Air Force officials did not assess network components—such as switches, routers, servers, and firewalls—for cybersecurity vulnerabilities prior to network connection and throughout the components (device) life cycle. The AFAA reviewed network components purchased between September 2016 and October 2017 at 14 Air Force locations and found that personnel did not account for network components, assess component configurations for vulnerabilities, monitor component configurations for continued cybersecurity, or develop corrective action plans for unmitigated vulnerabilities. [redacted]

- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

~~(FOUO)~~ The AFAA determined that these conditions occurred for the following reasons:

- Communication squadron commanders did not develop controls to detect when personnel did not document network component purchases in the system of record or to ensure that personnel documented corrective action plans to remediate or mitigate vulnerabilities at the component (device) level.
- ~~(FOUO)~~ [redacted]
- The Air Force Enterprise Authorizing Official approved a continuous monitoring strategy that used automated tools to scan for vulnerabilities at the network level, but the strategy did not include monitoring tools and techniques for devices at the device level.

~~(FOUO)~~ Consequently, the AFAA identified 2,334 cybersecurity vulnerabilities, 387 of which were on the Air Force's highest risk categories list—[redacted] that, if left unmitigated, would allow adversaries to gain control of network devices, divert network traffic, intercept sensitive information, or cause denial of service attacks.[37] Identifying cybersecurity vulnerabilities and taking action to mitigate them improves network security and enables Air Force officials to reduce network risks to acceptable levels. Without effective cybersecurity assessments, Air Force personnel introduced unnecessary risks to Air Force networks.

The AFAA made six recommendations to improve the cybersecurity of network component purchases. For example, the AFAA recommended that the Air Force Deputy CIO direct communication squadron commanders to develop and implement a process to ensure personnel document network component purchases in the Air Force system of record upon receipt. The AFAA also recommended that the Air Force Deputy CIO instruct communication commanders to develop and document a process to ensure that personnel create corrective action plans to remediate or mitigate identified network component (device) vulnerabilities. Air Force officials agreed with the recommendations. As of September 30, 2019, all six recommendations remained open.

Asset Management Category Takeaway

We determined that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Asset Management category. For example, the 20 reports issued and one testimony provided to Congress identified cybersecurity risks specific to software application rationalization processes and accountability of DoD systems, networks, and data. By implementing the recommendations identified in the reports, the DoD can improve its ability to track, manage, and secure its assets—data, personnel, devices, and systems.

Risk Assessment Category

We determined for that there were 18 reports issued that identified risks relating to the Risk Assessment category. The NIST Cybersecurity Framework defines the Risk Assessment category outcomes as those actions that allow an organization to understand the cybersecurity risks to its operations (including mission, functions, image, or reputation), assets, and workforce. The reports identified risks related

[37] ~~(FOUO)~~ [redacted]

to such things as unknown weapon system cybersecurity vulnerabilities, delays in conducting circuit reauthorizations, and inconsistent implementation of information system risk categorization.[38]

The 18 reports included recommendations to DoD officials to establish or update policies, procedures, or controls to correct the risks related to cybersecurity risk assessment. The following reports identified cybersecurity risks related to the Risk Assessment category and the impact of the risks.

(FOUO) [redacted]

(FOUO) [redacted]

- (FOUO) [redacted]

[38] (FOUO) [redacted]

[39] (FOUO) [redacted]

- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

GAO Report No. GAO-19-128, "Weapon Systems Cybersecurity, DoD Just Beginning to Grapple with Scale of Vulnerabilities," October 2018

The GAO determined that, during operational testing conducted between 2012 and 2017, DoD test teams routinely found mission-critical cyber vulnerabilities that adversaries could compromise in nearly all weapon systems that were under development. The GAO reviewed DoD cybersecurity test reports that demonstrated the ability of the DoD test teams to gain unauthorized access to weapon systems in a short amount of time using relatively simple tools and techniques. These reports showed that the DoD test teams were able to take full or partial control of systems and largely operate undetected. In some cases, system operators were unable to effectively respond to the intrusions. The DoD test team reports also indicated that the weapon system cybersecurity vulnerabilities were due, in part, to basic issues such as poor password management and unencrypted communications. Further, the DoD test reports showed that multiple weapon systems used commercial or open source software, but officials did not change the default password when the software was installed, which allowed test teams to look up the password on the internet and gain administrator privileges for that software.

In addition, the GAO determined that it was likely that the DoD did not know the full scale of its weapon system vulnerabilities because, for a number of reasons, the DoD tests were limited in scope and sophistication. These limitations occurred, in part, because the DoD cybersecurity assessment test teams did not reflect the full range of threats that weapon systems may face in operation and the nature of the tests imposed limitations on the DoD test teams that did not apply to potential adversaries. For example, the GAO reported that DoD officials

stated that the DoD test teams conducted most cybersecurity assessments over a few days to a few weeks; whereas, a determined adversary could spend months or years targeting systems. DoD officials also explained that, because DoD test teams had a limited amount of time with a system, they may have looked for the easiest or most effective way to gain access and did not identify all vulnerabilities that an adversary could exploit. Weapon systems cybersecurity assessments may also be limited in the types of attacks that are performed so entire categories of vulnerabilities are not currently addressed in some cyber assessments. Although there are practical reasons for limiting the duration and scope of cybersecurity assessments, these limitations mean that the DoD may not fully understand the extent of weapon system cyber vulnerabilities.

Furthermore, the GAO found that the DoD took several steps to improve weapon systems cybersecurity, including issuing and revising policies and guidance to better incorporate cybersecurity considerations. These steps were focused on improving the DoD's understanding of its weapon systems' vulnerabilities, determining how to mitigate risks from those vulnerabilities, and informing future development of more secure systems. For example, the DoD was compiling existing vulnerability information and conducting new tests to provide information about the cybersecurity posture of individual systems, concentrating mostly on fielded systems. The GAO concluded that these assessments were important because some of the systems did not undergo cybersecurity testing prior to fielding and the DoD did not have a permanent process in place to periodically assess the cybersecurity of fielded systems. The GAO did not make recommendations but planned to continue to evaluate this issue.

Risk Assessment Category Takeaway

We determined that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Risk Assessment category. For example, the 18 reports issued identified cybersecurity risks specific to the insufficient processes to successfully implement the DoD RMF and the limited emphasis on cybersecurity during weapon system design and development. By implementing the recommendations identified in the report, the DoD will improve its identification of critical cybersecurity workforce gaps and ability to fill those gaps. In addition, the DoD is taking steps to improve its understanding and mitigation of the DoD weapon systems' vulnerabilities.

Protect Function

We determined that there were 32 issued reports—22 unclassified and 10 classified—and one testimony provided to Congress that identified risks relating to the Protect function, primarily within the Information Protection Processes and Procedures and the Awareness and Training categories. The Protect function includes those activities that assist the organization to develop and implement appropriate safeguards to ensure delivery of critical services. These reports and testimony identified risks and weaknesses relating to the Protect function—such as incomplete continuity of operations plans and insufficient sanitization and disposal of information technology equipment—that impacts DoD operations, resources, and assets. Table 4 provides the NIST Cybersecurity Framework categories under the Protect function and the corresponding cybersecurity outcomes.

Table 4. NIST Cybersecurity Framework Categories for the Protect Function

Function	Category	Cybersecurity Outcomes
Protect	Identity Management and Access Control	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
	Awareness and Training	The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.*
	Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

*NIST defines industrial control systems as an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems that control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

Source: NIST Cybersecurity Framework.

~~(FOUO)~~ Additionally, some of the reports identified improvements (expanded access controls) or cybersecurity risks made in three of the other categories under the Protect function—Identity Management and Access Control, Data Security, and Protective Technology. Examples of the risks identified in reports that are not summarized in the Protect function sections below include the following:

- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

We determined that there were no reports issued or testimonies provided to Congress that identified risks related to the Maintenance category, which includes the maintenance and repair of organizational assets, such as industrial control systems, consistent with policies and procedures.[40] To address cybersecurity risk in the Protect function, the DoD must implement controls, such as issuing, managing, and verifying the identities and credentials of authorized users, that support the ability to limit or contain the impact of potential cybersecurity incidents.

The following sections provide examples from unclassified reports that identified risks and improvements in the two main categories identified under the Protect function—Information Protection Processes and Procedures and Awareness and Training. In each category we provide the number of reports that identified risks, the definition of the category, and an overview of the cybersecurity risks with

[40] Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

associated causes and examples. For each example, we provide a summary of the report's findings, causes, effects, and status of the recommendations made along with an example of a recommendation.

Information Protection Processes and Procedures Category

We determined that there were 20 issued reports that identified risks relating to the Information Protection Processes and Procedures category. The NIST Cybersecurity Framework defines Information Protection Processes and Procedures category outcomes as those that allow an organization to maintain and use security policies, processes, and procedures to manage protection of its information systems and assets. The reports identified risks related to such things as insufficient controls over information system configuration management, contingency planning, and the disposal of hard drives including personally identifiable information.

The 20 reports included recommendations for DoD officials to ensure the implementation of controls such as requiring network assets to be under a configuration management plan, updating contingency plans as required, and training property custodians on the proper sanitization and disposal of computers and associated hard drives. The reports also identified improvements made in the Information Protection Processes and Procedures category. The following reports identified cybersecurity risks related to the Information Protection Processes and Procedures category and the impact of the risks.

DODIG Report No. DODIG-2018-136, "Followup Audit on Application Level General Controls for the Defense Cash Accountability System," July 10, 2018

The DoD OIG conducted this followup audit in response to the Defense Cash Accountability System, Program Office's request to verify whether the implemented corrective actions addressed the issues identified in a 2017 DoD OIG report and if the corresponding recommendations could be closed.[41] The DoD OIG previously reported in FY 2017 that Defense Finance and Accounting Service officials did not implement effective application general controls for the Defense Cash Accountability System in FY 2016. Specifically, the DoD OIG found general control weaknesses related to training of information system security officers, periodically reviewing users' access to sensitive financial data, updating information system contingency plans, and tracking authorized system changes. The DoD OIG made

[41] DoD OIG issued Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016. The DoD uses the Defense Cash Accountability System to process and report its disbursement and collections of funds to the U.S. Treasury and the DoD. The Defense Cash Accountability System receives financial transaction data recorded from various DoD entity feeder systems, validates the accuracy of the data, and sends the data to appropriate DoD entity accounting systems. Monthly, the Defense Cash Accountability System processes more than 2 million transactions and 600 reports with over 14,000 files processed.

20 recommendations to address the identified internal control weaknesses associated with security management, access controls, configuration management, and contingency planning. Defense Finance and Accounting Service officials agreed with all 20 recommendations; thus, the recommendations were resolved but remained open.

In the 2018 followup audit, the DoD OIG determined that Business Enterprise Information Services Office officials implemented corrective actions that improved the design and operating effectiveness of several key application-level general controls related to security management, access controls, configuration management, and contingency planning. This occurred because Business Enterprise Information Services officials developed, revised, disseminated, and implemented policies and procedures, and trained personnel on the Defense Cash Accountability System specific controls. As a result of effective implementation of nine controls—such as information awareness training, user access, contingency planning coordination, and vulnerability management planning—the DoD OIG closed 11 of the 20 recommendations made in the FY 2017 report.

Additionally, the DoD OIG found that Business Enterprise Information Services Office officials made control design improvements to their access and configuration management controls, meeting the intent of four additional recommendations, which were subsequently closed. Improvements consisted of reviewing system level agreements with DISA account representatives, training personnel on how to periodically review user access, and monitoring user access (exception reports). However, the DoD OIG determined that Business Enterprise Information Services Office personnel had not yet verified that these new controls were operating fully as intended and additional actions were needed to demonstrate the successful implementation of these controls. As a result, the DoD OIG issued four new recommendations to verify that the new controls were operating effectively. In addition, the DoD OIG redirected one prior recommendation from Business Enterprise Information Services Office personnel to Defense Finance and Accounting Service Enterprise Shared Services personnel to verify and track that Master Data Table changes are authorized, configured, and operating effectively.[42]

Although these control enhancements closed 15 recommendations from the prior report, the Business Enterprise Information Services Office still needed to make additional improvements to security management, configuration management, and contingency planning controls to close the remaining 5 recommendations. For example, the DoD OIG determined that Business Enterprise Information Services Office officials still needed to require that system access requests matched

[42] Master Data Tables are sensitive data used to perform edits, verifications, and validations of data.

the level of access users were assigned in the Defense Cash Accountability System and that users still required access. The DoD OIG also determined Business Enterprise Information Services Office officials need to ensure that only authorized changes were made to the system's production environment and coordinate with DISA to schedule and perform an annual test of the system's contingency plan.

As a result, selected controls were not working effectively to minimize the risk that users accessed the Defense Cash Accountability System without authorization or correct level of privileges. In addition, the control weaknesses identified could circumvent existing controls, which were operating as intended. Without proper controls over application-level general controls, the Defense Cash Accountability System is vulnerable to availability interruptions and lost or incorrectly processed data. Losing the capacity to process, retrieve, and protect electronically maintained data can significantly impair and diminish the DoD's ability to accomplish its mission and process reliable financial data.

Consequently, the DoD OIG determined that 5 of the 20 prior recommendations remained open, 4 recommendations were reissued, and 1 recommendation was redirected from the FY 2017 report. Furthermore, the DoD OIG made five additional recommendations to address these issues. For example, the DoD OIG recommended that the Director of Business Enterprise Information Services and Other Systems at the Defense Finance and Accounting Service review and verify that privileged user reviews are conducted within consistent timeframes from the end of each quarter. Defense Finance and Accounting Service officials and DISA officials agreed with 9 of the 10 recommendations, and partially agreed with 1 recommendation. As of September 30, 2019, one recommendation remained open.

AFAA Report No. F2019-0006-O10000, "Cyber Asset Remanence Security," June 7, 2019

The AFAA determined that Air Force property custodians at all four locations reviewed did not ensure hard drives were removed or sanitized prior to disposition for 98 of 714 computers examined. Of the 98 hard drives, 59 contained data prohibited or exempt from disclosure by public law, including personally identifiable information—social security numbers, birth dates, cell phone numbers—and other protected information. For example, the AFAA found the following based on an extensive review of three hard drives:

- 234 medical records with protected health information detailing medical care provided, laboratory results, and medical diagnoses;
- 624 documents that contained personally identifiable information such as rosters with social security numbers, birth dates, addresses, cell phone numbers, and other family members' names and addresses; and

- 67 documents labeled as for official use only, indicating the information was protected from public release.

Furthermore, the AFAA found more than 2,200 unsanitized hard drives that were stored loosely in a box at three Air Force Bases even though the property custodians certified that the devices were sanitized.

This occurred because the accountable property officers did not train property custodians on proper sanitization and disposal of computers and associated hard drives in accordance with NIST standards.[43] As a result, Air Force property custodians were turning in computers with unsanitized hard drives to the Defense Logistics Agency for further use. Properly sanitizing electronic media prevents the reconstruction or disclosure of sensitive data, such as personally identifiable and protected health information by individuals without proper clearance or the need to know. For example, sanitized computers and hard drives are made available by the Defense Logistics Agency for further use to other federal agencies, authorized nonfederal recipients, and surplus customers (nonprofit organizations) or are offered to the general public for re-sale. Therefore, an individual or non-profit organization could acquire computers and hard drives that contained personally identifiable and protected health information and data prohibited or exempt from disclosure by public law.

The AFAA recommended that the Air Force Deputy CIO, in coordination with installation commanders, ensure NIST requirements relating to remanence security were enforced by accountable property officers and accountable property officers train property custodians on proper sanitization and disposal of computers and associated hard drives. The Air Force Deputy CIO agreed with all recommendations. As of September 30, 2019, the two recommendations remained open.

Information Protection Processes and Procedures Category Takeaway

We determined that DoD continues to face significant challenges in managing cybersecurity risks associated with the Information Protection Processes and Procedures category. For example, the 20 reports identified risks specific to configuration management and sanitizing media. Although the DoD took corrective actions to update policies, train personnel, and develop contingency plans to protect the DoD's systems and data, additional actions are needed such as ensuring that contingency plans are tested annually. By implementing the recommendations identified in the reports, the DoD can improve its ability manage risks to the DoD enterprise.

[43] Remanence security involves sanitization actions taken to prevent the reconstruction or disclosure of sensitive information from an information system's electronic media.

Awareness and Training Category

~~(FOUO)~~ We determined that there were 17 issued reports and one testimony provided to Congress that identified risks relating to the Awareness and Training category. The NIST Cybersecurity Framework defines the Awareness and Training category as cybersecurity awareness education and training provided to the organization's personnel and partners that is needed to the perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. [redacted]

~~(FOUO)~~ The 17 reports included recommendations to DoD officials [redacted] The following report identified cybersecurity risks related to the Awareness and Training category and the impact of the risks.

GAO Report No. GAO-19-142SU, "DOD Training, U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force," November 6, 2018[44]

~~(FOUO)~~ [redacted]

The GAO also determined that the DoD began to shift focus from building CMF teams to maintaining a trained CMF. Although the DoD developed a transition plan for the CMF that transfers foundational training responsibility from USCYBERCOM to the Military Services, the Army and Air Force did not establish timeframes for validating that their foundational courses met the USCYBERCOM standards. Furthermore, the Military Services' plans did not identify the number of personnel or teams and the specific training activities needed to complete each phase of training to maintain the appropriate CMF team sizing and deployment

[44] GAO Report No. GAO-19-362, "U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force," March 6, 2019, is the unclassified version of the GAO Report No. GAO-19-142SU, which includes the same information and additional information that is classified as ~~For Official Use Only.~~

of personnel across CMF teams. In addition, USCYBERCOM did not have a plan to establish required independent assessors to ensure the consistency of collective CMF training. Lastly, USCYBERCOM had not established master training task lists for foundational training courses, which the Military Services needed to prepare appropriate course equivalency standards.[45]

As a result, the DoD needs to focus on maintaining a ready CMF and addressing gaps in its training plans and structure. If not properly addressed, these issues could contribute to training inefficiency and unnecessarily long timeframes for training personnel. Thereby, leading to teams being certified to different standards, and contributing to inconsistent personnel skill levels and inefficient use of training resources.

The GAO made eight recommendations, including that:

- the Army and Air Force identify timeframes for validating foundational CMF courses,
- the Military Services develop CMF training plans with specific personnel requirements, and
- USCYBERCOM develop and document a plan establishing independent assessors to evaluate training.

The DoD agreed with all eight recommendations. As of September 30, 2019, the eight recommendations remained open.

Awareness and Training Takeaway

~~(FOUO)~~ We determined that despite numerous improvements reported by the DoD over the past year, there were 17 recently issued cybersecurity-related reports and one testimony that demonstrate that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Awareness and Training category. For example, these reports and testimony identified risks specific to training and [redacted] By implementing the recommendations identified in the reports, the DoD will enable the cybersecurity workforce to perform its duties and responsibilities to protect the DoD's data, systems, and infrastructure.

[45] USCYBERCOM assesses the prior experience of CMF personnel to meet training requirements through a process known as individual training equivalency. This process allows personnel to be exempted from specific training courses by showing that they have already met the learning objectives of the course through their prior experience. Training task lists are a key set of standards that the Military Services use to prepare course equivalency standards.

Detect Function

We determined that there were 10 reports—5 unclassified and 5 classified—that identified risks relating to the Detect function, primarily within the Security Continuous Monitoring category. The Detect function includes those activities that assist the organization to develop and implement appropriate activities to identify the occurrence of a cybersecurity event. These reports identified risks and weaknesses relating to the Detect function—such as the identification and mitigation of vulnerabilities and that ensuring officials understood their cybersecurity roles and responsibilities—that affects the DoD Components' ability to fully implemented established policies and procedures to effectively manage cybersecurity risks that impacted the DoD operations, resources, and assets. Table 5 provides the NIST Cybersecurity Framework categories under the Detect function and the corresponding cybersecurity outcomes.

Table 5. NIST Cybersecurity Framework Categories for the Detect Function

Function	Category	Cybersecurity Outcomes
Detect	Anomalies and Events	Anomalous activity is detected and the potential impact of events is understood.
	Security Continuous Monitoring	The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.

Source: NIST Cybersecurity Framework.

~~(FOUO)~~ Additionally, some of the reports identified risks in the other two categories under the Detect function—Anomalies and Events and Detection Processes. [redacted] To address cybersecurity risks related to the Detect function, the DoD must implement controls and processes, such as monitoring external service provider activity, to detect cybersecurity incidents.

The following section provides examples from unclassified reports that identified risks in the main category identified under the Detect function—Security Continuous Monitoring. In each category we provide the number of reports that identified risks, the definition of the category, and an overview of the

cybersecurity risks with associated causes and examples. For each example, we provide a summary of the report's findings, causes, effects, and status of the recommendations made along with an example of a recommendation.

Security Continuous Monitoring Category

We determined that there were eight reports issued that identified risks relating to the Security Continuous Monitoring category. The NIST Cybersecurity Framework defines Security Continuous Monitoring category outcomes as those that allow an organization to monitor its information systems and assets to identify cybersecurity events and verify the effectiveness of protective measures. The reports identified risks related to such things as the identification and mitigation of vulnerabilities and detecting unauthorized wireless devices, services, and technologies.

The eight reports included recommendations to DoD officials to establish or update policies, procedures, or controls to correct the risks associated with mitigating the vulnerabilities identified during CCRIs and conducting active searches for unauthorized wireless devices. The following reports identified cybersecurity risks related to the Security Continuous Monitoring category and the impact of the risks.

DODIG Report No. DODIG-2018-137, "Command Cyber Readiness Inspections at Air Force Squadrons," July 11, 2018

~~(FOUO)~~ The DoD OIG determined that Air Force Squadrons did not correct all system and network vulnerabilities identified during CCRIs even though all five Air Force squadrons reviewed passed their respective FY 2015 CCRIs. The DoD OIG verified in FY 2017 that squadrons did not subsequently correct or mitigate all vulnerabilities identified during the FY 2015 CCRIs. [redacted]

[46] ~~(FOUO)~~ [redacted]

- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

[47] ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted] Therefore, known vulnerabilities that remain unmitigated could provide the ability to exploit the vulnerabilities and obtain unauthorized access to Air Force networks and potentially the DODIN. Once access is obtained, unauthorized users could compromise the systems and install programs; view, change, or delete data; or create new accounts with full user rights.

The DoD OIG made three recommendations, including a recommendation for the Air Force to develop a process to ensure that vulnerabilities identified during routine vulnerability scanning and CCRIs were mitigated within the USCYBERCOM required compliance timeframes and in accordance with DoD Instruction 8510.01 requirements. The Chief, Information Dominance and CIO, Office of the Secretary of the Air Force, neither agreed nor disagreed, stating that the Air Force continued to improve its CCRI processes and procedures through multiple related efforts. The Chief stated that the Air Force was developing policy to describe and standardize the teamwork, roles, and responsibilities needed for cyber inspection readiness and compliance across the Air Force, including mitigating CCRI-identified vulnerabilities. The Chief estimated that the policy would be completed by October 1, 2018. As of September 30, 2019, all three recommendations remained open.

Naval Audit Service Audit Report N2019-0029, "Followup on Information Security Within the U.S. Marine Corps," April 2, 2019

~~(FOUO)~~ [redacted]

(FOUO) [redacted]

(FOUO) [redacted]

Security Continuous Monitoring Takeaway

We determined that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Security Continuous Monitoring category. For example, the eight reports identified cybersecurity risks specific to the identification and mitigation of vulnerabilities and detecting unauthorized wireless devices, services, and technologies. By implementing the recommendations identified in the reports, the DoD will improve its ability to monitor and detect cybersecurity incidents, and verify the effectiveness of protective measures.

Respond Function

We determined that there were eight reports issued—four unclassified and four classified—that identified risk relating to the Respond function, primarily within the Mitigation category. The Respond function includes those activities that assist the organization to develop and implement appropriate activities to take action regarding a detected cybersecurity incident. These reports identified risks and weaknesses relating to the Respond function—such as developing plans of action and milestones to remediate or mitigate known vulnerabilities—

that impact an organization's ability to manage and take action to address detected cybersecurity incidents. Table 6 provides the NIST Cybersecurity Framework categories under the Respond function and the corresponding cybersecurity outcomes.

Table 6. NIST Cybersecurity Framework Categories for the Respond Function

Function	Category	Cybersecurity Outcomes
Respond	Response Planning	Response processes and procedures are executed and maintained to ensure response to detected cybersecurity incidents.
	Communications	Response activities are coordinated with internal and external stakeholders (for example, external support from law enforcement agencies).
	Analysis	Analysis is conducted to ensure effective response and support recovery activities.
	Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities.

Source: NIST Cybersecurity Framework.

Additionally, some of the reports identified risks in the other three categories under the Respond function—Response Planning, Communications, and Analysis. Examples of reports that are not summarized in the Respond function sections below include the following:

- The DoD did not implement a GAO recommendation to maintain a database that identifies National Guard cyber capabilities that could support civil authorities during a cyber incident. As a result, the DoD did not have full visibility into the National Guard's cyber capabilities that could provide support during a cyber incident.
- ~~(FOUO)~~ [redacted]

- ~~(FOUO)~~ [redacted]

We determined that there were no reports issued or testimonies provided to Congress that identified risks related to the Improvements category, which addresses actions taken to incorporate lessons learned into response plans and to update response strategies. To address cybersecurity risks related to the Respond function, the DoD must mitigate known vulnerabilities in a timely manner and establish processes and procedures for sharing cybersecurity-related information to effectively respond to incidents.

The following section provides an example from an unclassified report that identified risks in the Mitigation category under the Respond function. In each category we provide the number of reports that identified risks, the definition of the category, and an overview of the cybersecurity risks with associated causes and examples. For each example, we provide a summary of the report's findings, causes, effects, and status of the recommendations made along with an example of a recommendation.

Mitigation Category

We determined that there were four issued reports that identified risks relating to the Mitigation category. The NIST Cybersecurity Framework defines Mitigation category outcomes as activities that are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. The reports identified risks related to the identification and successful remediation of vulnerabilities or developing a plan of action and milestones for vulnerabilities that could not be immediately mitigated.

The four reports included recommendations to DoD officials to remediate identified vulnerabilities in a timely manner and provide all JRSS operators with training. The following report describes how Mitigation risks affected the DoD operations and the impact of the risks.

DODIG Report No. DODIG-2019-089, "Audit of the DoD's Implementation of the Joint Regional Security Stacks," June 4, 2019

~~(FOUO)~~ The DoD OIG determined that the DoD's implementation of the JRSS was not fully achieving the expected outcomes of the DoD's Joint Information Environment initiatives to implement regional security.[48] Although implementing the JRSS was reducing the footprint and number of enemy attack vectors to the DODIN, the DoD OIG also determined that JRSS was not achieving other intended Joint Information Environment outcomes for implementing regional security such as [redacted]

This occurred because DoD officials did not ensure that all JRSS tools met users' needs and that JRSS operators were trained prior to JRSS deployment. Without achieving all intended outcomes, the JRSS is not operationally effective, secure, and sustainable and thus, the DoD may not achieve the Joint Information Environment vision, including greater security of the DoDIN.

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted] Without adequate security safeguards for the JRSS, the weaknesses could prevent network defenders from obtaining the information necessary to make timely decisions, and could lead to unauthorized access to the DoDIN and the destruction, manipulation, or compromise of the DoD data.

[48] The Joint Information Environment contains 10 capability objectives, one of which is to implement regional security. The expected outcomes of implementing regional security are to provide timely access to trusted cyber situational awareness, reduce the number of paths an adversary can use to gain access to the DODIN, and improve the DODIN security posture.

[49] ~~(FOUO)~~ [redacted]

~~(FOUO)~~ As a result, the DoD OIG made five recommendations, [redacted] The DoD agreed with three recommendations, partially agreed with one recommendations, and disagreed with one recommendation. As of September 30, 2019, all five recommendations remained open.

Mitigation Takeaway

~~(FOUO)~~ We determined that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Mitigation category. For example, the four issued reports that identified cybersecurity risks specific to the identification and successful remediation of vulnerabilities or developing a plan of action and milestones for vulnerabilities that could not be immediately mitigated. By implementing the recommendations identified in the reports, [redacted]

Recover Function

We did not identify any issued reports or testimonies provided to Congress by the DoD OIG, GAO, or the other DoD oversight organizations between July 1, 2018, and June 30, 2019, pertaining to the Recover function. The Recover function includes activities that help an organization recover to normal operations, in a timely manner, to reduce the impact from a cybersecurity incident. The Recover function consists of three categories—recovery planning, improvements, and communications. Table 7 provides the NIST Cybersecurity Framework categories under the Recover function and the corresponding cybersecurity outcomes.

Table 7. NIST Cybersecurity Framework Categories for the Recover Function

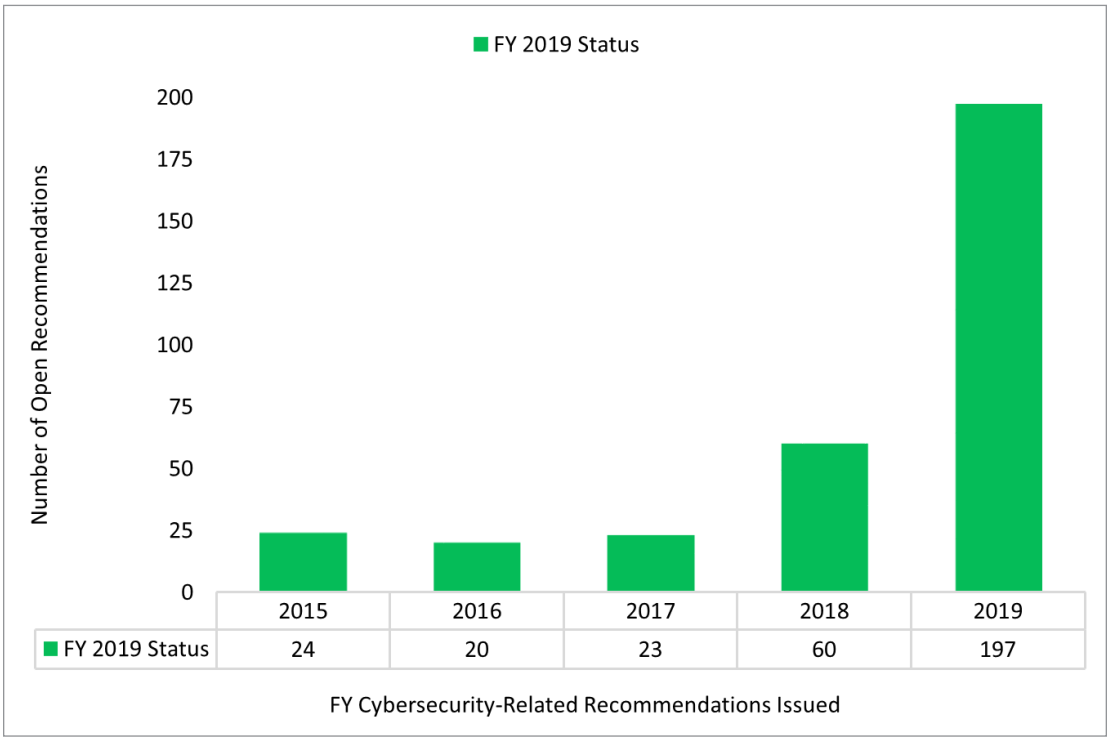
Function	Category	Cybersecurity Outcomes
Recover	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
	Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications	Restoration activities are coordinated with internal and external parties (for example, coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams, and vendors).

Source: NIST Cybersecurity Framework.

Open Cybersecurity-Related Recommendations

Although we are not making new recommendations to DoD management in this summary report, it is vital to the DoD's overall cybersecurity posture that management implement timely and comprehensive corrective actions to address the open recommendations. As of September 30, 2019, we identified that the DoD needs to take action to close the 330 open DoD cybersecurity-related recommendations—297 unclassified and 33 classified—from reports dating as far back as FY 2011. The DoD OIG, GAO, and the other DoD oversight organizations are responsible for following-up on the status of corrective actions taken in response to oversight reports and the associated recommendations as well as determining whether open recommendations remain relevant. Figure 3 shows the age of all open cybersecurity-related recommendations by fiscal year of report issuance.

Figure 3. Open Cybersecurity-Related Recommendations by Fiscal Year



Note: The 2019 recommendations were recently issued and, therefore, DoD management may not have had sufficient time to implement all necessary actions for closure. Also, the FY 2015 data above represents the cumulative total number of open recommendations for FY 2011 through FY 2015.

Source: The DoD OIG.

The DoD OIG, GAO, and the other DoD oversight organizations made 24 cybersecurity related recommendations prior to FY 2016 that remained open, which dated as far back as FY 2011. Of the 24 recommendations:

- the DoD OIG had 16 recommendations directed toward the Under Secretary of Defense for Personnel and Readiness, the Deputy Chief Financial Officer, the DoD CIO, the Army, and the Navy related to physical access control systems, data loss prevention, controls and audit trails for information system processes, cloud computing strategies and information system configuration, that have remained open since FY 2015 or earlier;
- the GAO had one recommendation directed toward the DoD to work with the Department of Veterans Affairs to resolve problems with collaboration sites' incompatible processes, such as computer security training, that has remained open since FY 2012;
- ~~(FOUO)~~ [redacted]
- ~~(FOUO)~~ [redacted]

Recommendation Status for Reports Included in This Summary Report

The DoD OIG, GAO, and the other DoD oversight organizations made 296 DoD cybersecurity-related recommendations in 46 reports—33 unclassified and 13 classified—issued from July 1, 2018, through June 30, 2019. Of the 296 DoD recommendations made, 197 remained open as of September 30, 2019, with the majority related to the Identify and Protect functions.

For the 197 open cybersecurity-related recommendations, DoD management agreed with 115 of them; as of September 30, 2019, however, 82 recommendations remained unresolved.[50] The unresolved DoD recommendations consisted of the following:

- 57 recommendations to which management did not provide a response;
- 13 recommendations with which management partially agreed;

[50] Open recommendations can be either resolved or unresolved. Resolved recommendations are those that DoD management has agreed to implement, but for which management has not yet completed agreed-upon actions. Unresolved recommendations are those that DoD management has not agreed to implement or proposed actions that will not address the intent of the recommendation.

- 11 recommendations for which management provided actions that partially addressed the identified issues; and
- 1 recommendation with which management disagreed.

For example, the DoD partially agreed with a recommendation made in Report No. DODIG-2019-089, "Audit of the DoD's Implementation of the Joint Regional Security Stacks." The DoD OIG recommended that the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the DoD CIO, establish or revise guidance to require the DoD Components to follow the same requirements when developing a technology refresh that will exceed an established cost threshold, as required for new acquisitions under DoD Instruction 5000.02.[51] The DoD officials agreed with the intent of the recommendation to rigorously manage technology refresh programs, but not to establish a fixed threshold that would require all such programs to be managed as "new programs." Specifically, the Assistant Secretary of Defense for Acquisition stated that the Under Secretary of Defense for Acquisition and Sustainment was developing policy to guide future DoD information systems and commercial-off-the-shelf hardware acquisitions, and would consider the intent of the recommendation when developing the policy. In response, the DoD OIG stated that although the Assistant Secretary partially agreed with the recommendation, the proposed actions to establish guidance for DoD information systems and commercial-off-the-shelf acquisitions did not describe how the new guidance would include procedures that the DoD Components should take when developing a technology refresh that will exceed an established cost threshold. Therefore, the DoD OIG determined that this recommendation was unresolved at the time the report was issued; however, the DoD OIG requested additional comments from the DoD on this recommendation in response to the final report. As of September 30, 2019, this recommendation was resolved but remained open.

The DoD has numerous open recommendations that have remained unaddressed, which date as far back as FY 2011. DoD management must determine whether the recommendations are still relevant and ensure that the DoD not only takes timely and appropriate corrective actions to address its open recommendations, but also ensures that it implements effective risk management practices to reduce cybersecurity risks affecting the DODIN and all business and military operations.

[51] DoD Instruction 5000.02, "Operation of the Adaptive Acquisition Framework," January 23, 2020. A technology refresh is an incremental insertion of newer technology to improve reliability, improve maintainability, reduce cost, and add minor performance enhancements.

Other DoD Cybersecurity-Related Issues

In FY 2018 and FY2019, the DoD OIG and independent public accounting firms' auditors conducted the first two audits of the DoD's financial statements consisting of more than 20 audits each year of the DoD and its components financial statements. These audits included assessments of information technology systems that the DoD used to process financial transactions that are reported on financial statements.[52] A significant function of financial statement audits is reviewing information technology and cyber security. Auditors reported that the DoD and 13 of its Components had a material weakness related to financial management systems, as well as their information technology environments. As of December 31, 2019, the DoD had more than 1,500 open information technology NFRs as a result of the FY 2018 and FY 2019 financial statement audits.[53] We determined that some of the information technology NFRs identified weaknesses relating to the NIST Cybersecurity Framework.

Within the DoD, financial transactions are rarely completed using only one information technology system from the point of initiation to the point that the transactions are reported on the financial statements. Many of the systems crucial to financial management and reporting are also used for operational purposes and are not owned and operated by the DoD Components that rely on them for financial reporting. During FY 2019, auditors identified 247 systems relevant to internal controls over financial reporting. For example, the Military Services depend on over a dozen information technology systems that are owned and operated by the other DoD Components to process and record contract payments. During the financial statement audits, testing of DoD information technology systems and interfaces between information technology systems can identify vulnerabilities in those systems and result in recommendations to improve the DoD's cyber security.

In FY 2018 and again in FY 2019, auditors determined that the DoD had a material weakness related to the DoD financial management systems and information technology. Specifically, the DoD had wide-ranging financial management system weaknesses that could prevent the DoD from collecting and reporting financial and performance information that is accurate, reliable, and timely.[54] Auditors found

[52] Within the DoD, financial transactions are rarely completed using only one information system from the point a transaction is initiated until it is reported on the financial statements. For example, in 2016, the DoD reported that it had nearly 400 separate systems that processed accounting data.

[53] DoD OIG Report, "Understanding the Results of the Audit of the DoD FY 2019 Financial Statements," January 28, 2020.

[54] Weaknesses and inefficiencies in financial processes are categorized as a material weakness, significant deficiency, or control deficiency based on the severity of the weakness. Control deficiencies are provided to management throughout the audit, and a summary of the control deficiencies is provided after the completion of the audit.

significant cybersecurity control deficiencies affecting systems reviewed across multiple DoD Components. For example, the auditors identified that the DoD did not:

- appropriately restrict access rights and responsibilities according to segregation of duties policy (Identity Management and Access Control category);
- terminate user access in a timely manner when users left the organization (Identity Management and Access Control category);
- implement controls to identify unintentional or unauthorized changes made to applications, databases, or data (Information Protection Processes and Procedures category); or
- perform reconciliations between systems to verify the completeness and accuracy of data being transferred (Data Security).

As of December 31, 2019, the DoD had more than 1,500 information technology NFRs that remained open. These open information technology NFRs comprised more than 800 FY 2018 NFRs (of the more than 1200 issued) and 750 new NFRs in FY 2019.[55] To address the large number of open information technology NFRs, the DoD stated that it was developing a business plan that will outline the number of systems that impact financial reporting that the it plans to retire, resulting in a reduced footprint of systems that impact financial reporting. This plan included decreasing the number of legacy information technology systems by 51 during FY 2019 to FY 2023.

~~(FOUO)~~ Furthermore, the DoD took actions to close nearly 400 information technology NFRs that auditors issued in FY 2018. The auditors verified the DoD management actions taken as part of their FY 2019 audits. Specifically, the Army implemented 65 percent of its information technology corrective action plans related to findings from the FY 2018 audit. [redacted]

[55] NFRs are used communicate to management in a timely manner any identified weaknesses and inefficiencies in financial processes, the impact of these weaknesses and inefficiencies, the reason the weaknesses and inefficiencies exist, and recommendations to management on how to correct the weaknesses and inefficiencies.

The following sections provide examples from information technology NFRs that identified risks related to the Identity Management and Access Control, the Information Protection Processes and Procedures, the Protective Technology, and the Data Security categories under the Protect function. For each information technology NFR example, we provide a summary of the NFR's findings, the cause, the effect, and the recommendations as they pertain to the NIST Cybersecurity Framework category as well as the status of the NFR.

Identity Management and Access Control Category (Protect Function)

The auditors identified cybersecurity risks related to the Identity Management and Access Control category in the NFRs. The NIST Cybersecurity Framework defines Identity Management and Access Control category outcomes as those that allow an organization to limit access to physical and logical assets and associated facilities to authorized users, processes, and devices, and to manage access consistent with the assessed risk of unauthorized access to authorized activities and transactions.

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

[56] ~~(FOUO)~~ [redacted]

[57] ~~(FOUO)~~ [redacted]

Information Protection Processes and Procedures Category (Protect Function)

The auditors identified cybersecurity risks related to the Information Protection Processes and Procedures category in the NFRs. The NIST Cybersecurity Framework defines Information Protection Processes and Procedures category outcomes as those that allow an organization to maintain and use security policies, processes, and procedures to manage protection of its information systems and assets.

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

Protective Technology (Protect Function)

The auditors identified cybersecurity risks related to the Protective Technology category in the NFRs. The NIST Cybersecurity Framework defines Protective Technology category outcomes as those that allow an organization to manage technical security solutions to ensure that the security and resilience of systems and assets are consistent with related policies, procedures, and agreements.

[58] ~~(FOUO)~~ [redacted]

(FOUO) [redacted]

(FOUO) [redacted]

Data Security (Protect Function)

The auditors identified cybersecurity risks related to the Data Security category in the NFRs. The NIST Cybersecurity Framework defines Data Security category outcomes as those that allow an organization to manage its information and records (data) consistent with its risk strategy to protect the confidentiality, integrity, and availability of information.

[59] (FOUO) [redacted].

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

Takeaways From Financial Statement Information Technology NFRs

During the FY 2018 and the FY 2019 DoD financial statement audits, the auditors identified the need for the DoD to develop and implement more effective internal controls for 247 information technology systems that process transactions for financial reporting, including controls to manage user accounts, monitor user activities, and secure the systems from other cybersecurity risks for systems that process financial transactions. In FY 2019, the auditors reported that the DoD and 13 of its Components had a material weakness related to financial management systems, as well as their information technology environment. As of December 31, 2019, the DoD had more than 1,500 open information

[60] ~~(FOUO)~~ [redacted]

[61] ~~(FOUO)~~ [redacted]

technology NFRs as a result of the FY 2018 and FY 2019 financial statement audits. We determined that some of these NFRs identified weaknesses relating to the NIST Cybersecurity Framework.

Ineffective system controls can result in significant risk to DoD assets. For example, payments and collections could be lost, stolen, or duplicated as a result of weak information technology controls. Implementing the recommended actions included in these NFRs will better enable the DoD to improve its overall reliance on the accuracy and completeness of financial data. In addition, improving internal controls for information technology systems that process financial transactions can improve not only financial management but also the overall cybersecurity of the DODIN and can better assist in protecting against and rapidly responding to cyber threats across its various networks and systems.

Appendix A

Scope and Methodology

We conducted this summary work from January 2019 through April 2020. We followed generally accepted government auditing standards except for the standards of planning and evidence because the report summarizes previously released reports.

For this summary, we identified unclassified and classified reports issued and testimony provided to Congress by the DoD OIG, GAO, and the other DoD oversight organizations between July 1, 2018, and June 30, 2019. Specifically, we coordinated with members of the Defense Council on Integrity and Efficiency Technology Committee, the Defense Intelligence Community agencies, and the GAO to obtain the unclassified and classified reports for review and consideration when writing this summary report. We reviewed the findings and recommendations in each report and compared them against the five NIST Cybersecurity Framework function outcomes to determine if the findings and recommendations related to the NIST Cybersecurity Framework, but did not review the supporting documentation for any of the reports. Because the summarized reports contained recommendations related to the identified cybersecurity risks, this summary report does not contain additional recommendations. Lastly, we planned to include classified appendixes to this report for information directly pertaining to the classified reports issued during the period. Although we include the number of classified reports issued in our discussion of the NIST Cybersecurity Framework and categories, we did not issue classified appendixes summarizing the specific findings and results of those reports due to impact of the coronavirus disease–2019 on classified processing requirements.

Use of Computer-Processed Data

We did not use computer-processed data for this summary report.

Prior Coverage

During the last 5 years, the DoD OIG issued five reports summarizing cybersecurity risks identified in 117 audit reports (unclassified and classified) issued and three testimonies made by the DoD OIG, GAO, and the other DoD oversight organizations. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

The following reports are For Official Use Only (FOUO) and can be obtained through the Freedom of Information Act Requestor Service website at https://www.dodig.mil/foia/submit-foia/.

DoD OIG

Report No. DODIG-2019-044, "Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018," January 9, 2019 (Report is FOUO)

> The DoD OIG identified 24 reports—20 unclassified and 4 classified—issued by the DoD OIG, GAO, and the DoD oversight community from July 1, 2017, through June 30, 2018, relating to the DoD cybersecurity risks and improvements. Specifically, the DoD OIG identified that DoD Components implemented corrective actions necessary to improve system weaknesses identified in issued reports summarized in the FY 2017 cybersecurity summary report, but also concluded that recently issued cybersecurity reports indicate that the DoD still faces challenges in managing cybersecurity risks to its network. As of September 30, 2018, 266 DoD cybersecurity-related recommendations, remained open, dating as far back as 2008.

Report No. DODIG-2018-126, "DoD Cybersecurity Weaknesses Identified in Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017," June 13, 2018 (Report is FOUO)

> The DoD OIG identified 29 unclassified reports issued and one testimony provided to Congress by the DoD OIG, GAO, and the DoD oversight community from July 1, 2016, through June 30, 2017. The DoD OIG identified that the DoD still faces challenges in key cybersecurity risk areas pertaining to Identify, Protect, and Detect functions. These three functions are designed to help an organization to understand its cybersecurity risks, implement appropriate safeguards, and identify cybersecurity events.

Report No. DODIG-2017-034, "DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2015, Through July 31, 2016," December 13, 2016 (Report is FOUO)

> The DoD OIG identified 21 unclassified reports issued by the DoD OIG, GAO, and the DoD oversight community from August 1, 2015, through July 31, 2016 that addressed a wide range of cybersecurity weaknesses within DoD systems and networks. These reports most frequently cited cybersecurity weaknesses in the areas of risk management, identity and access management, security and privacy training, contractor system security, and configuration management. While the DoD prioritized funding its cyber strategy, cybersecurity will continue to remain a significant management challenge. As recent audit

reports identified, the DoD continues to struggle with ensuring that all aspects of its information security program were adequately implemented. As of July 31, 2016, 138 DoD cybersecurity-related recommendations remained open.

Report No. DODIG-2015-180, "DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2014, Through July 31, 2015," September 25, 2015 (Report is FOUO)

The DoD OIG identified 20 unclassified reports issued and one testimony provided to Congress by the DoD OIG, GAO, and the DoD oversight community from August 1, 2014, through July 31, 2015 that addressed a wide range of cybersecurity weaknesses within DoD systems and networks. Reports issued during the reporting period most frequently cited cybersecurity weaknesses in the categories of Risk Management, Identity and Access Management, and Contingency Planning. As of July 31, 2015, 136 DoD cybersecurity-related recommendations remained open.

Report No. DODIG-2014-126, "DoD Cybersecurity Weaknesses as Reported in Audit Reports Issued From August 1, 2013, Through July 31, 2014," September 26, 2014 (Report is FOUO)

The DoD OIG identified 23 unclassified reports and one testimony made by the DoD OIG, GAO, and the DoD oversight community from August 1, 2013, through July 31, 2014 that addressed a wide range of cybersecurity weaknesses within DoD systems and networks. Reports issued during the reporting period most frequently cited cybersecurity weaknesses in the categories of Risk Management, Contingency Planning, and Identity and Access Management. As of July 31, 2014, 151 DoD cybersecurity-related recommendations remained open.

Appendix B

Unclassified and Classified Reports and Testimonies Regarding DoD Cybersecurity

Issued Reports

GAO

1. Report No. GAO-19-58, "Cloud Computing, Agencies Have Increased Usage and Realized Benefits, but Cost and Savings Data Need to Be Better Tracked," April 4, 2019
2. Report No. GAO-19-366SP, "Priority Open Recommendations: Department of Defense," March 28, 2019
3. Report No. GAO-19-136, "DoD Space Acquisitions: Including Users Early and Often in Software Development Could Benefit Programs," March 18, 2019
4. Report No. GAO-19-144, "Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs," March 12, 2019
5. Report No. GAO-19-114R, "Cybersecurity: Federal Agencies Met Legislative Requirements for Protecting Privacy When Sharing Threat Information," December 6, 2018
6. Report No. GAO-19-142SU, "U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force," November 6, 2018 (Report is FOUO)[62]
7. Report No. GAO-19-128, "Weapon Systems Cybersecurity, DOD Just Beginning to Grapple with Scale of Vulnerabilities," October 9, 2018
8. Report No. GAO-18-497SPC, "Long-Range Emerging Threats Facing the U.S. Identified by Federal Agencies," September 28, 2018 (Report is SECRET//NOFORN)[63]
9. Report No. GAO-18-622, "High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation," September 6, 2018
10. Report No. GAO-18-558, "Defense Infrastructure: Guidance Needed to Develop Metrics and Implement Cybersecurity Requirements for Utilities Privatization Contracts," September 4, 2018

[62] GAO Report No. GAO-19-362, "U.S. Cyber Command and Services Should Take Actions to Maintain a Trained Cyber Mission Force," March 6, 2019, is the unclassified version of the GAO Report No. GAO-19-142SU listed above.

[63] GAO Report No. GAO-19-204SP, "National Security: Long-Range Emerging Threats Facing the United States As Identified by Federal Agencies," December 13, 2018 is the unclassified version of GAO-18-497SPC listed above.

GAO (Cont'd)

11. Report No. GAO-18-93, "Federal Chief Information Officers: Critical Actions Needed to Address Shortcomings and Challenges in Implementing Responsibilities," August 2, 2018

DoD OIG

12. Report No. DODIG-2019-097, "Followup to DODIG-2018-068, Evaluation of Oversight of Privileged Users Within the Army's Intelligence Component," June 19, 2019 (Report is SECRET)
13. Report No. DODIG-2019-089, "Audit of the DoD's Implementation of the Joint Regional Security Stacks," June 4, 2019 (Report is FOUO)
14. Report No. DODIG-2019-072, "Audit of Consolidated Afloat Networks and Enterprise Services Security Safeguards," April 8, 2018 (Report is SECRET)
15. Report No. DODIG-2019-063, "Followup Audit on the Military Department Security Safeguards Over SIPRNet Access Points," March 18, 2019 (Report is SECRET//NOFORN)
16. Report No. DODIG-2019-037, "DoD Management of Software Applications," December 13, 2018 (Report is FOUO)
17. Report No. DODIG-2019-034, "Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information," December 10, 2018 (Report is SECRET//NOFORN)
18. Report No. DODIG-2019-016, "DoD Actions to Implement the Cybersecurity Information Sharing Act of 2015 Requirements," November 8, 2018 (Report is FOUO)
19. Report No. DODIG-2018-163, "DoD Cyber Incident Handling Program for Mission-Critical Control Systems," September 28, 2018 (Report is SECRET)
20. Report No. DODIG-2018-154, "DoD Information Technology System Repositories," September 24, 2018
21. Report No. DODIG-2018-143, "Air Force Space Command Supply Chain Risk Management of Strategic Capabilities," August 14, 2018 (Report is FOUO)
22. Report No. DODIG-2018-137, "Command Cyber Readiness Inspections at Air Force Squadrons," July 11, 2018 (Report is FOUO)
23. Report No. DODIG-2018-136, "Followup Audit: Application Level General Controls for the Defense Cash Accountability System," July 10, 2018

Army Audit Agency

24. ~~(FOUO)~~ [redacted]
25. ~~(FOUO)~~ [redacted]
26. ~~(FOUO)~~ [redacted]
27. ~~(FOUO)~~ [redacted]

Naval Audit Service

28. Report No. N2019-0032, "Implementation of Naval Computer and Telecommunications Station Far East Continuity of Operations Planning Capability," May 7, 2019 (Report is FOUO)
29. Report No. N2019-0029, "Follow Up on Information Security Within the U.S. Marine Corps," April 2, 2019 (Report is FOUO)
30. Report No. N2019-0007, "Management of Personally Identifiable Information at Selected Commander, U.S. Pacific Fleet Activities," December 17, 2018 (Report is FOUO)
31. Report No. N2019-0002, "Department of the Navy's Insider Threat Program," October 12, 2018 (Report is FOUO)
32. Report No. N2018-0055, "Navy Military Human Resources Systems Business Enterprise Architecture," September 25, 2018 (Report is FOUO)

Air Force Audit Agency

33. Report No. F2019-0006-O10000, "Cyber Asset Remanence Security," June 7, 2019
34. Report No. F2019-0005-O10000, "Cybersecurity of Integrated Tactical Warning Attack Assessment Weapon Systems," May 7, 2019 (Report is FOUO)
35. Report No. F2019-0004-O10000, "Cloud Computing Security" March 28, 2019
36. Report No. F2019-0002-O10000, "Cybersecurity of Network Component Purchases," January 22, 2019 (Report is FOUO)
37. Report No. F2019-0001-O10000, "Information Technology Investment Portfolio Suite Accuracy," October 24, 2018
38. Report No. F2018-0004-L30000, "Network-Centric Solutions-2 Contract Management," July 3, 2018 (Report is FOUO)

Other DoD Agencies

39. National Security Agency OIG Report No. AU-18-0006, "Audit of NSA Corporate Authorization Service (CASPORT)," June 24, 2019 (Report is TOP SECRET)
40. DISA Report No. 17_IG21_001_400_AA, "Audit of Secret Internet Protocol Router Network (SIPRNet) Access Controls," April 16, 2019 (Report is SECRET//NOFORN)
41. Defense Intelligence Agency OIG Report No. 2018-2004, "Evaluation of DIA's Five Eye Engagement for Cyber Intelligence," March 15, 2019 (Report is TOP SECRET)
42. Defense Intelligence Agency OIG Report No. 2018-2010, "Evaluation of Counterintelligence Operations in the Cyber Domain," January 31, 2019 (Report is TOP SECRET)
43. DISA Report No. 16_IG21_004_300_AA, "Audit of DISA's Compliance With Contracting Requirements for Cyber Safeguards of Covered Defense Information," September 27, 2018
44. National Security Agency OIG Report No. AU-18-0009, "Review of the Designation of Individuals to Fill Systems Security Plan (SSP) Critical Roles," September 27, 2018 (Report is TOP SECRET)
45. National Security Agency OIG Report No. AU-17-0006A, "Audit of Nuclear Command and Control Systems," September 26, 2018 (Report is TOP SECRET)
46. National Security Agency OIG Report No. JT-8-0002, "Inspection of Information Technology Inspection of Alaska Mission Operations Center (AMOC), July 16-20, 2018," March 11, 2019 (Report is TOP SECRET)

Testimonies Made

GAO

1. GAO-19-641T, "Information Technology, Implementation of GAO Recommendations Would Strengthen Federal Agencies' Acquisitions, Operations, and Cybersecurity Efforts," June 26, 2019
2. GAO-19-367T, "Army Readiness, Progress and Challenges in Rebuilding Personnel, Equipping, and Training," February 6, 2019
3. GAO-18-645T, "High Risk Series, Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation," July 25, 2018

Appendix C

NIST Cybersecurity Framework Functions

Function	Corresponding Cybersecurity Activities
Identify	Develop the organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services.
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Source: NIST Cybersecurity Framework.

NIST Cybersecurity Framework Categories

Function	Category	Cybersecurity Outcomes
Identify	Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and risk strategy.
	Business Environment	The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance	The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
	Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.

NIST Cybersecurity Framework Categories (Cont'd)

Function	Category	Cybersecurity Outcomes
Protect	Identity Management and Access Control	Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
	Awareness and Training	The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures	Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance	Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.*
	Protective Technology	Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
Detect	Anomalies and Events	Anomalous activity is detected and the potential impact of events is understood.
	Security Continuous Monitoring	The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes	Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Respond	Response Planning	Response processes and procedures are executed and maintained to ensure response to detected cybersecurity incidents.
	Communications	Response activities are coordinated with internal and external stakeholders (for example, external support from law enforcement agencies).
	Analysis	Analysis is conducted to ensure effective response and support recovery activities.
	Mitigation	Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements	Organizational response activities are improved by incorporating lessons learned from current and previous detection and response activities.

NIST Cybersecurity Framework Categories (Cont'd)

Function	Category	Cybersecurity Outcomes
Recover	Recovery Planning	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
	Improvements	Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications	Restoration activities are coordinated with internal and external parties (for example, coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams, and vendors).

* NIST defines industrial control systems as an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems that control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

Source: NIST Cybersecurity Framework.

Appendix D

Reports and Testimonies Identifying Risks by NIST Cybersecurity Framework Category

~~(FOUO)~~	NIST Cybersecurity Framework (by Function and Category)																		
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
Agency Report No.	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
GAO																				
GAO-18-93	x		x																	
GAO-18-558						x														
GAO-18-622	x	x	x			x	x	x		x				x		x				
GAO-19-128	x		x	x																
GAO-19-142SU								x												
GAO-19-114R			x	x																
GAO-19-144	x		x																	
GAO-19-136				x		x														
GAO-19-366SP			x					x												
GAO-19-58										x										~~(FOUO)~~

Reports and Testimonies Identifying Risks by NIST Cybersecurity Framework Category (Cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																		
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
DoD OIG																				
DODIG-2018-136	x		x		x	x	x	x		x		x								
DODIG-2018-137	x	x	x	x	x		x			x				x						
DODIG-2018-143			x	x		x			x											
DODIG-2018-154	x		x					x												
DODIG-2019-016			x				x			x							x			
DODIG-2019-037	x		x																	
DODIG-2019-089			x	x			x	x	x			x			x			x	x	
Army Audit Agency																				
~~(FOUO)~~ [redacted]	[redacted]																			
~~(FOUO)~~ [redacted]																				
[redacted]																				
[redacted]																				

Reports and Testimonies Identifying Risks by NIST Cybersecurity Framework Category (Cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																			
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
Naval Audit Service																				
~~(FOUO)~~ N-2018-0055	[redacted]																			
~~(FOUO)~~ N-2019-0002																				
~~(FOUO)~~ N-2019-0007																				
~~(FOUO)~~ N-2019-0029																				
~~(FOUO)~~ N-2019-0032																				
Air Force Audit Agency																				
~~(FOUO)~~ F2018-0004-L30000	[redacted]																			
F2019-0001-O10000																				
~~(FOUO)~~ F2019-0002-O10000																				
F2019-0004-O10000																				
~~(FOUO)~~ F2019-0005-O10000																				
F2019-0006-O10000																				

Reports and Testimonies Identifying Risks by NIST Cybersecurity Framework Category (Cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																		
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
Other DoD Organizations																				
16_IG21_004_300_AA						X														
Unclassified Reports Subtotal	17	2	24	14	6	8	8	13	7	12	0	2	0	4	1	1	1	2	1	0
Classified Reports Subtotal	3	0	5	4	1	0	8	4	2	8	0	4	1	4	3	1	0	0	3	0
Testimonies*	1							1												
Grand Total	**21**	**2**	**29**	**18**	**7**	**8**	**16**	**18**	**9**	**20**	**0**	**6**	**1**	**8**	**4**	**2**	**1**	**2**	**4**	**0** ~~(FOUO)~~

Note: Totals do not equal the number of reports identified because one report may cover more than one NIST Cybersecurity Framework Category. The table does not include the Recover function because we did not identify any reports issued that addressed these areas.

*The totals for testimonies represent only one testimony—GAO-19-367T. The other two testimonies made—GAO-19-641T and GAO-18-645T—discuss the same issues identified in GAO Report No. GAO-18-622, which we included in this summary report.

Source: The DoD OIG

Appendix E

Open Recommendations by NIST Cybersecurity Framework Category

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																			
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
GAO																				
GAO-18-93	1		1																	
GAO-18-558																				
GAO-18-622																				
GAO-19-58																				
GAO-19-114R																				
GAO-19-128																				
GAO-19-136				2		2														
GAO-19-142SU								8												
GAO-144	2		2																	
GAO-19366SP																				~~(FOUO)~~

Open Recommendations by NIST Cybersecurity Framework Category (Cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																		
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category			
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
DoD OIG																				
DODIG-2018-136							1	1												
DODIG-2018-137	2	2	3	2	3		2			3				1						
DODIG-2018-143			3	3		3			2											
DODIG-2018-154																				
DODIG-2019-016			8				1			1							8			
DODIG-2019--037	3		3																	
DODIG-2019-089			4	1				4	2			2			2			1	1	
Army Audit Agency																				
~~(FOUO~~ [redacted]	[redacted]																			
~~(FOUO)~~ [redacted]																				
[redacted]																				
[redacted]																				

Open Recommendations by NIST Cybersecurity Framework Category (Cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																		
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
Naval Audit Service																				
~~(FOUO)~~ N-2018-0055	[redacted]																			
~~(FOUO)~~ N-2019-0002																				
~~(FOUO)~~ N-2019-0007																				
~~(FOUO)~~ N-2019-0029																				
~~(FOUO)~~ N-2019-0032																				

Open Recommendations by NIST Cybersecurity Framework Category (Cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																		
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
Air Force Audit Agency																				
~~(FOUO)~~ F2018-0004-L30000	[redacted]																			
F2019-0001-O10000																				
~~(FOUO)~~ F2019-0002-O10000																				
F2019-0004-O10000																				
~~(FOUO)~~ F2019-0005-O10000																				
F2019-0006-O10000																				

Open Recommendations by NIST Cybersecurity Framework Category (Cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																			
	Identify Function Category						Protect Function Category						Detect Function Category			Respond Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness and Training	Data Security	Information Protection Processes and Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes	Response Planning	Communications	Analysis	Mitigation	Improvements
Other DoD Organizations																				
16_IG21_004_300_AA																				
Unclassified Reports Subtotal	23	2	53	23	11	8	11	27	14	26	0	3	0	5	2	0	8	6	1	0
Classified Reports Subtotal	10	0	8	15	0	0	77	24	45	50	0	41	0	50	39	0	0	0	51	0
Grand Total	**33**	**2**	**61**	**38**	**11**	**8**	**88**	**51**	**59**	**76**	**0**	**44**	**0**	**55**	**41**	**0**	**8**	**6**	**52**	**0** ~~(FOUO)~~

Note: Totals do not equal the number of recommendations identified because one recommendation may cover more than one NIST Cybersecurity Framework Category. The table does not include the Recover function categories because we did not identify any reports issued that addressed these areas.

Source: The DoD OIG.

Acronyms and Abbreviations

AAA	Army Audit Agency
AFAA	Air Force Audit Agency
CCRI	Command Cyber Readiness Inspection
CIO	Chief Information Officer
CISA	Cyber Information Sharing Act
CMF	Cyber Mission Force
DISA	Defense Information Systems Agency
DODIN	Department of Defense Information Network
GAO	Government Accountability Office
JRSS	Joint Regional Security Stacks
NFR	Notices of Findings and Recommendations
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
RMF	Risk Management Framework
USCYBERCOM	U.S. Cyber Command

Whistleblower Protection
U.S. Department of Defense

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

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

~~FOR OFFICIAL USE ONLY~~

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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

~~FOR OFFICIAL USE ONLY~~