Report No. DODIG-2021-034

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 11, 2020

Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2019, Through June 30, 2020

~~Controlled by: Office of the Secretary of the Air Force~~
~~Controlled by: Deputy Chief Information Officer~~
~~POC:~~ [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2019, Through June 30, 2020

December 11, 2020

Objective

The objective of this summary report was to: (1) summarize unclassified and classified reports and testimonies regarding DoD cybersecurity that the DoD Office of Inspector General (OIG), the Government Accountability Office (GAO), and other DoD oversight organizations issued from July 1, 2019 through June 30, 2020 concerning DoD cybersecurity; (2) identify cybersecurity trends; and (3) identify the open DoD cybersecurity-related recommendations.

We issue this summary report to identify DoD cybersecurity trends 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 implementing changes, as appropriate.

Background

Federal agencies are required to use the NIST Cybersecurity Framework to manage their cybersecurity risk. The NIST Cybersecurity Framework consists of five functions—Identify, Protect, Detect, Respond, and Recover—representing high-level cybersecurity activities that provide a strategic view of the risk management cycle for identifying, assessing, and responding to risk. In addition, the five functions include 23 associated categories, such as "Asset Management" or "Detection Process," that provide desired cybersecurity outcomes. Each of the

Background (cont'd)

23 categories has up to 12 subcategories that further divide the categories into specific outcomes of technical and management activities, such as "data-at-rest is protected" or "notifications from detection systems are investigated."

The DoD also uses the Risk Management Framework which provides an integrated enterprise-wide decision structure for managing cybersecurity risk for DoD information technologies.

Summary

This year's report summarizes the results of the 44 DoD cybersecurity-related reports issued—33 unclassified and 11 classified—by the DoD OIG, GAO, and the other DoD oversight organizations from July 1, 2019, through June 30, 2020. We did not identify any testimonies made by the DoD oversight community or GAO regarding DoD cybersecurity risks during this period.

Despite the improvements made by the DoD over the past year, recently issued cybersecurity reports demonstrated that the DoD continued to face significant challenges in managing cybersecurity risks to its systems and networks. For example, the DoD has made improvements regarding the NIST Cybersecurity Framework categories of Risk Management Strategy (Identify function) and Communications (Respond function) by utilizing Risk Management Framework processes and sharing cybersecurity information with stakeholders. However, risks remain in managing the DoD's cybersecurity activities regarding 20 of the 23 NIST Cybersecurity Framework categories. The majority of the risks and weaknesses identified in the 44 reports we reviewed related to the categories of Governance (Identify function), Identity Management and Access Control (Protect function), Risk Assessment (Identify function), and the Information Protection Processes and Procedures (Protect function).

Results in Brief

Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2019, Through June 30, 2020

Summary (cont'd)

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

- know the extent that practices to protect DoD networks from key cyber attack techniques were implemented because DoD Components did not establish procedures to monitor implementation of key initiatives;
- establish internal controls to validate whether organizations with oversight responsibilities enforced information technology asset management policy, identified and monitored excess information technology hardware asset inventories, or managed the re-distribution of excess information technology hardware inventories; or
- implement cybersecurity measures and document system security parameters in accordance with DoD guidance and maintained outdated cybersecurity documentation such as an outdated Plan of Action and Milestones.

Furthermore, we determined that the DoD Components implemented corrective actions necessary to close 197 of 656 cybersecurity-related recommendations from issued reports included in this summary report and prior summary reports. However, as of August 2020, the DoD had 459 cybersecurity-related recommendations open, dating back to 2011.

In addition to the 44 reports issued from July 1, 2019 through June 30, 2020, we also reviewed the notices of findings and recommendations issued to the DoD as part of the agency financial statement audits. As of July 1, 2020, the DoD had 1,710 open information technology notices of findings and recommendations (NFRs) as a result of the FY 2019 and FY 2020 financial statement audits.[1] The notices of findings and recommendations identified weaknesses regarding the (1) Identity Management and Access Control and (2) Information Protection Processes and Procedures categories under the Protect function of the NIST Cybersecurity Framework.

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 that address the open cybersecurity-related recommendations. Implementing corrective actions is necessary because DoD adversaries such as Russia, China, Iran, and North Korea; terrorist groups; hacktivists; and other malicious actors can exploit cybersecurity vulnerabilities to gain unauthorized access to systems and networks and use sensitive and classified information to collect intelligence, target DoD critical infrastructure, manipulate information, and conduct cyber attacks.

[1] Notices of findings and recommendations are used to 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

December 11, 2020

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Summary of Reports Issued Regarding Department of Defense Cybersecurity from July 1, 2019, Through June 30, 2020 (Report No. DODIG-2021-034)

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


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

Introduction

Objective

The objective of this summary report was to: (1) summarize unclassified and classified reports and testimonies regarding DoD cybersecurity that the DoD Office of Inspector General (OIG), the Government Accountability Office (GAO), and the other DoD oversight organizations issued from July 1, 2019, through June 30, 2020; (2) identify cybersecurity trends; and (3) identify the open DoD cybersecurity-related recommendations.[2]

We issue this summary report to identify DoD cybersecurity trends 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 implementing changes, as appropriate.

See Appendix A for a discussion of the scope and methodology and list of previously issued cybersecurity summary reports. See Appendix B for a list of the unclassified and classified reports summarized in this report. See Appendix C for a list of reports identifying cybersecurity risks by the NIST Cybersecurity Framework category. See Appendix D for a matrix of open recommendations organized by NIST Cybersecurity Framework function. See Appendix E for summaries of the identified classified (up to SECRET) cybersecurity reports.

Background

The DoD relies on cyberspace and cyber capabilities to perform its military and intelligence missions, as well as its business operations. Cyberspace is a global domain that consists of the Internet, telecommunications networks, and computer systems. The DoD needs to continuously assess and adapt its cyberspace capabilities to defend the DoD Information Network and the systems and networks of the DoD's partners and allies. According to the Deputy Secretary of Defense, as of November 2019, the DoD had more than 2,500 data centers, 355 cloud initiatives, 48,000 applications, 11,000 circuits, and 1,850 business systems. In addition, the Deputy Secretary of Defense stated that standardizing and modernizing the DoD's

[2] 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. Closed recommendations are recommendations where DoD management took corrective action, and the action taken was verified by the oversight organization.

networks, services, and data centers, and leveraging enterprise capabilities and security functions eliminates duplicative systems and reduces DoD's exposure to cyber risks and threats.[3]

The scope and pace of malicious cyber activity from foreign countries, such as Russia, China, Iran, and North Korea continues to increase. These actors can use the Internet to exploit cyber vulnerabilities and gain unauthorized access and use of sensitive and classified information to threaten U.S. interests. According to the Commander of U.S. Cyber Command:

- the Chinese Communist Party's use of political repression and economic coercion—particularly through forced tech transfers and state-sponsored commercial espionage—harms U.S. interests and undermines the sovereignty of our allies and partners;
- Russia's efforts to undermine western institutions and to intimidate its neighbors have showcased its willingness to launch destructive cyber operations and pervasive influence campaigns;
- Iran has conducted disruptive cyber attacks against U.S. companies and partners, and employs similar tactics, along with information operations, to push its own narrative across the Middle East; and
- North Korea uses cyber operations to steal currency that it would otherwise be denied under international sanctions.[4]

DoD Risk Management Framework

Cybersecurity risk management is the activities taken 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.[5] According to the Instruction, all DoD information technology must be assigned to, and governed by, a DoD Component cybersecurity program that manages risk commensurate with the importance of the 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).[6] The instruction mandates the use of the RMF for all DoD information technologies and is consistent with the principles established in the NIST Cybersecurity Framework.[7]

[3] Statement by Mr. David L. Norquist, Deputy Secretary of Defense, Testimony before the U.S. Senate Armed Service Committee, Subcommittee on Readiness, November 20, 2019.

[4] Statement by General Paul M. Nakasone, Commander of U.S. Cyber Command, Before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities, March 4, 2020.

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

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

[7] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018.

NIST Cybersecurity Framework

In February 2013, the President issued Executive Order 13636 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 within the U.S. identify, assess, and manage cyber risk.[8] In addition, the Cybersecurity Enhancement Act of 2014 required NIST to develop an approach to help critical infrastructure owners and operators identify, assess, and manage cyber risk for critical infrastructure.[9]

To further 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. The Office of Management and Budget (OMB) also issued guidance in May 2017 to support Federal agencies in implementing Executive Order 13800 requirements.[10]

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.[11] Use of the Framework allows an organization to communicate using a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. The 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.

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 will occur and the potential resulting impacts. Organizations should then determine the acceptable level of risk for achieving their organizational objectives and express this as their risk tolerance. After establishing the risk tolerance, organizations can then prioritize cybersecurity activities and make informed decisions about cybersecurity expenditures.

[8] Exec. Order No. 13,636, 3 CFR sec. 7 (2013).

[9] Public Law 113-274, "Cybersecurity Enhancement Act of 2014," December 18, 2014.

[10] Exec. Order No. 13,800, 3 CFR sec. 1 (2017).

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

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 processes; instead, an organization can use its current process and apply the Framework to determine any gaps in its current cybersecurity risk approach and develop a roadmap to improvement. Using the 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.

Framework Functions, Categories, and Subcategories

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 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," while the Recover function activities 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, such as "Asset Management" or the "Detection Process," that provide desired cybersecurity outcomes. Each of the 23 categories has up to 12 subcategories that further divide the categories into specific outcomes of technical or management activities, including subcategories such as "data-at-rest is protected" or "notifications from detection systems are investigated." Table 1 lists the 5 functions and the 23 corresponding categories.

Table 1. NIST Cybersecurity Framework Functions and Categories

<table>
<tr><th>Function</th><th>Identify</th><th>Protect</th><th>Detect</th><th>Respond</th><th>Recover</th></tr>
<tr><td rowspan="8">Category</td><td>Asset Management</td><td>Identity Management and Access Control</td><td rowspan="2">Anomalies and Events</td><td rowspan="2">Response Planning</td><td rowspan="2">Recovery Planning</td></tr>
<tr><td>Business Environment</td><td>Awareness and Training</td></tr>
<tr><td>Governance</td><td>Data Security</td><td rowspan="2">Security Continuous Monitoring</td><td>Communications</td><td rowspan="2">Improvements</td></tr>
<tr><td>Risk Assessment</td><td>Information Protection Processes and Procedures</td><td>Analysis</td></tr>
<tr><td>Risk Management Strategy</td><td>Maintenance</td><td rowspan="2">Detection Processes</td><td>Mitigation</td><td rowspan="2">Communications</td></tr>
<tr><td>Supply Chain Risk Management</td><td>Protective Technology</td><td>Improvements</td></tr>
</table>

Source: NIST Cybersecurity Framework.

Summary

The DoD Continues to Face Challenges in Managing Cybersecurity Risks

This year's report summarizes the results of the 44 DoD cybersecurity-related reports issued—33 unclassified and 11 classified—by the DoD OIG, GAO, and the other DoD oversight organizations from July 1, 2019 through June 30, 2020.[12] We did not identify any testimony by the DoD oversight community or GAO regarding DoD cybersecurity risks during this period.

We determined that the DoD Components implemented corrective actions necessary to close 197 of the 656 cybersecurity-related recommendations from reports issued between July 1, 2019 and June 30, 2020 included in this summary report and prior summary reports.[13] Those corrective actions indicate progress in the DoD's efforts to mitigate or remediate risks and weaknesses to the DoD systems and networks. However, as of August 2020, the DoD still had 459 cybersecurity-related recommendations that remained open, dating back to 2011.[14]

We also determined that despite improvements made by the DoD, cybersecurity reports issued during the last year demonstrate that the DoD continues to face significant challenges in managing cybersecurity risks to its systems and networks. For example, our review of the reports identified that the DoD made improvements regarding the NIST Cybersecurity Framework categories of Risk Management Strategy (Identify function) and Communications (Respond function) by utilizing the RMF processes and sharing cybersecurity information with stakeholders. However, those same reports also identified risks related to 20 of the 23 NIST Cybersecurity Framework categories. The majority of the identified risks and weaknesses related to the categories of Governance (Identify function), Identity Management and Access Control (Protect function), Risk Assessment (Identify function), and the Information Protection Processes and Procedures (Protect function). See Appendix C for a list of reports issued during the last year that discussed cybersecurity risks by the NIST Cybersecurity Framework category.[15]

[12] See Appendix B for a list of all unclassified reports regarding the DoD cybersecurity issues during this period. See Appendix E for a list of all classified reports (up to SECRET) regarding the DoD cybersecurity issues during this period.

[13] See Appendix A for a list of prior cybersecurity summary reports issued by the DoD OIG over the last 5 years.

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

[15] We did not identify any reports made by the DoD oversight community or GAO regarding the Maintenance, Detection Processes, and Communications (Recover function) categories.

The risks generally occurred because DoD officials did not establish policies and procedures to implement minimum standards and necessary controls in accordance with DoD guidance. For example, the DoD did not:

- know the extent that practices to protect DoD networks from key cyber attack techniques were implemented because DoD Components did not establish procedures to monitor implementation of key initiatives; [16]
- establish internal controls to validate whether organizations with oversight responsibilities enforced information technology asset management policy, identified and monitored excess information technology hardware asset inventories, or managed the re-distribution of excess information technology hardware inventories;[17] and
- implement cybersecurity measures and document system security parameters in accordance with DoD guidance and maintain current cybersecurity documentation such as Plans of Action and Milestones.[18]

Additionally, as of July 1, 2020, the DoD had 1,710 open information technology notices of findings and recommendations (NFRs) as a result of the FY 2019 and FY 2020 financial statement audits.[19] We determined that the majority of the NFRs related directly to the concepts covered in the Protect function of the NIST Cybersecurity Framework including the categories of (1) Identity Management and Access Control and (2) Information Protection Processes and Procedures.

Lack of effective 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 the information technology NFRs will better enable the DoD to improve its overall reliance on the accuracy and completeness of financial-related data. In addition, improving internal controls for information technology systems that process financial transactions can improve financial management and the overall cybersecurity of the DoD Information Network.

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 the corrective actions recommended

[16] GAO Report No. GAO-20-241, "Cybersecurity: DoD Needs to Take Decisive Actions to Improve Cyber Hygiene," April 2020.

[17] Air Force Audit Agency Report No. F2020-0001-O10000, "Information Technology Hardware Asset Purchasing," October 11, 2019.

[18] Air Force Audit Agency Report No. F2019-0013-A00900, "Space Deconfliction System," July 17, 2019.

[19] NFRs are used to 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.

in the reports we summarized. DoD adversaries such as Russia, China, Iran, and North Korea; terrorist groups; hacktivists; and other independent malicious actors can exploit cybersecurity vulnerabilities to gain unauthorized access to systems and networks and use sensitive and classified information to collect intelligence, target DoD critical infrastructure, manipulate information, and conduct cyber attacks. The DoD must ensure that it 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. Therefore, it is vital to the DoD's overall cybersecurity posture that management implement timely and comprehensive corrective actions to address the open recommendations.

The DoD Took Actions to Improve DoD Cybersecurity

The DoD Components took corrective actions during the past year to close 197 DoD cybersecurity-related recommendations that addressed cybersecurity risks.[20] For example:

- In a FY 2018 report, the DoD OIG recommended that the Commander of U.S. Cyber Command revise guidance to clearly establish roles and responsibilities for oversight of cyber readiness inspections. To address the recommendation, the U.S. Cyber Command developed and issued an Execution Order that expanded the cybersecurity and cyber readiness focus of Command Cyber Readiness Inspections. As a result, U.S. Cyber Command's Command Cyber Readiness Inspections include a more comprehensive inspection process that encompasses mission assurance, operational readiness, risk identification, and cyber defense force abilities to mitigate vulnerabilities.
- In a FY 2019 report, the DoD OIG recommended that the U.S. Navy develop and implement a plan to verify that contractor correct weaknesses identified in the report related to using multifactor authentication. To address the recommendation, the Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center confirmed that a Navy contractor implemented multifactor authentication at all of its sites. The DoD OIG determined that the corrective actions taken by the Navy contractor met the intent of the recommendation. As a result, it is more difficult for an unauthorized user or malicious actor to assume the identity of an authorized user and to compromise the security of contractor owned networks and systems that maintain controlled unclassified information (CUI).

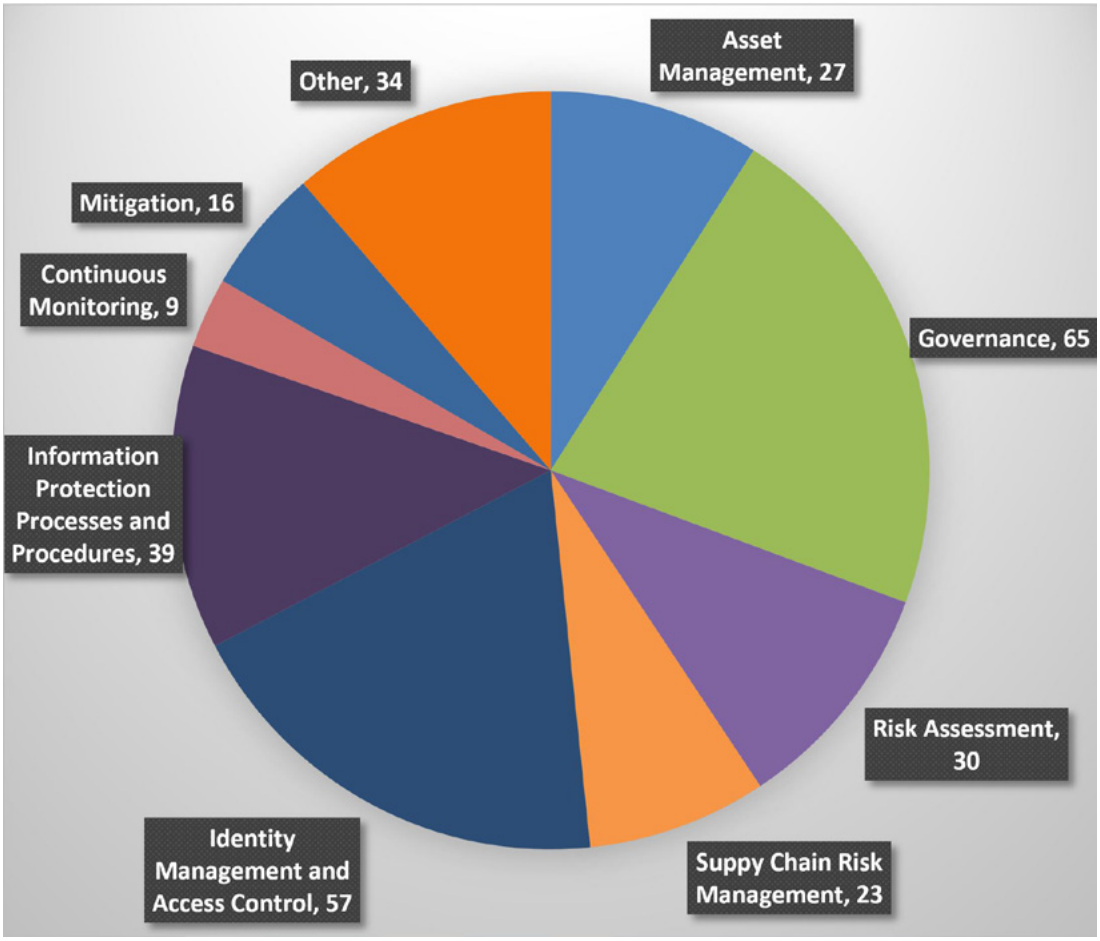
[20] As of August 2020, we identified that the DoD needs to take action to close the 459 open DoD cybersecurity-related recommendations—415 unclassified and 44 classified—from reports dating as far back as FY 2011.

- ~~(FOUO)~~ [redacted]
- In a FY 2017 report, the DoD OIG recommendation that the Chief Information Officers for Army Military Treatment Facilities develop a plan of action and milestones and take steps in a timely manner to mitigate known network vulnerabilities. To address the recommendation, the Defense Health Agency developed a plan that requires system owners to follow specific steps for addressing vulnerabilities. Additionally, the plan requires system owners to submit a security authorization for assessment to the Defense Health Agency for approval. As a result, the Defense Health Agency has increased assurance that its system owners are taking the appropriate steps to reduce or eliminate weaknesses regarding known network vulnerabilities.[21]

The corrective actions taken to address the report recommendations improved the DoD's compliance within the NIST categories of Identity Management and Access Control, Information Protection Processes and Procedures, and Governance. It is vital to the DoD's overall cybersecurity posture that management implement timely and comprehensive corrective actions that address the open cybersecurity-related recommendations. As of August 2020, the DoD had 459 open cybersecurity-related recommendations—415 unclassified 44 classified—that have been open since as far back as 2011. Figure 1 shows the number of open DoD cybersecurity-related recommendations from reports identified from July 1, 2019, through June 30, 2020, by NIST Cybersecurity Framework category.

[21] CUI is a designation for identifying unclassified information that requires proper safeguarding in accordance with Federal and DoD guidance.

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



Note: The "other" category comprises 10 of the 23 NIST Cybersecurity Framework categories. In addition, 5 of the 23 NIST Cybersecurity Framework categories did not have any related open recommendations. There were 215 open cybersecurity-related recommendations from reports issued between July 1, 2019 and June 30, 2020. Totals in Figure 1 do not equal 215 because one recommendation may cover more than one NIST Cybersecurity Framework function.

Source: The DoD OIG.

The DoD relies on information technology systems and networks to conduct its military operations and perform critical functions and the longer known cybersecurity vulnerabilities exist, the more the risks to the systems and networks increase. The vulnerabilities, if left unmitigated, can facilitate security incidents and cyber attacks that disrupt critical operations; lead to inappropriate access to and disclosure, modification, or destruction of sensitive information; and threaten national security.

Challenges Remain in Managing DoD Cybersecurity Risks

From July 1, 2019, through June 30, 2020, the DoD OIG, GAO, and other DoD oversight organizations issued 44 reports—33 unclassified and 11 classified—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), Risk Assessment (Identify function), Information Protection Processes and Procedures (Protect function), Awareness and Training (Protect function), and Identity Management and Access Control (Protect function).

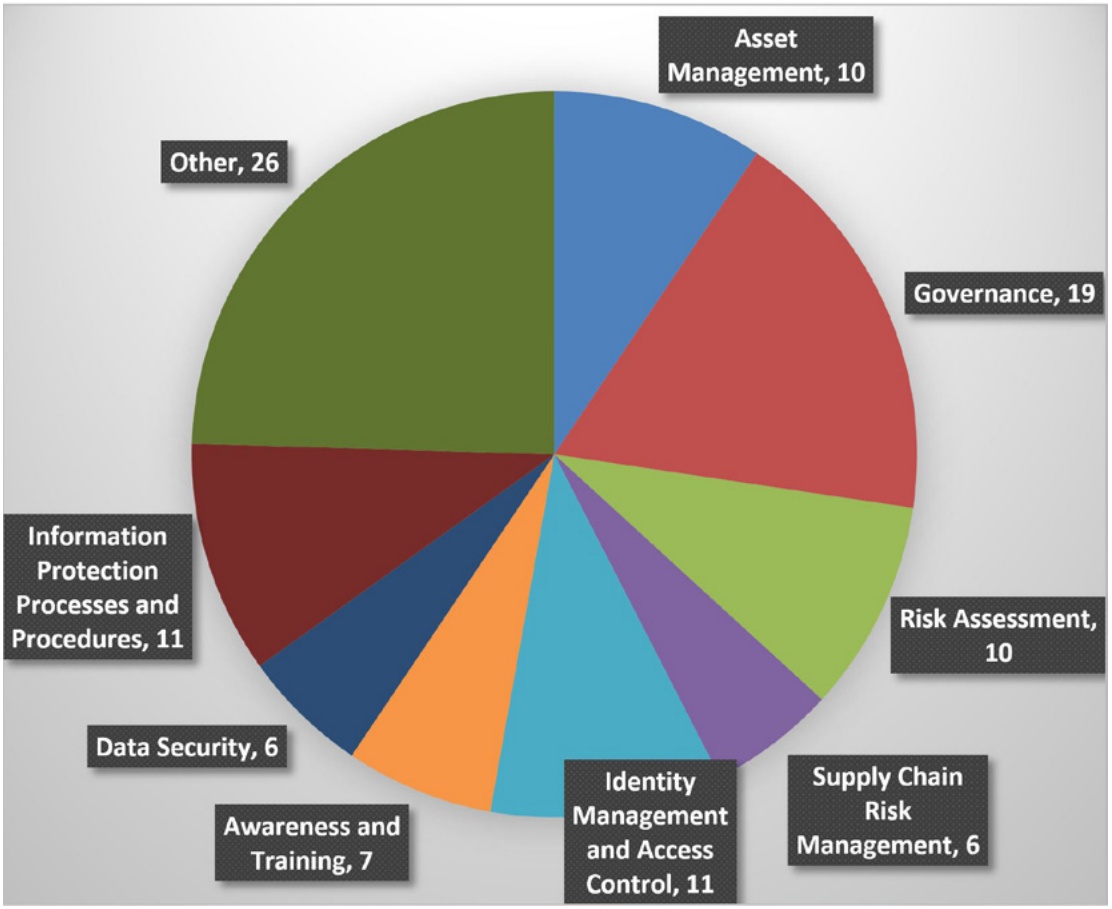
In this year's summary report, we determined that the category with the most identified risks or weaknesses was the Governance category, under the Identify function. Specifically, 19 of the reports issued generally identified that DoD officials did not have effective controls in place or take the steps needed to ensure that DoD Components fully implemented established policies and procedures. For example, in one report, the DoD OIG determined that DoD contractors did not consistently implement security controls in accordance with Federal and DoD requirements for safeguarding Defense CUI because DoD Component contacting offices and requiring activities did not establish processes to verify the contractors implemented minimum security controls required by NIST. Without adequate cybersecurity controls, the DoD is at a greater risk of its CUI being compromised by cyber attacks from malicious actors.

We also determined that other significant cybersecurity risks identified in the 44 reports issued relate to asset vulnerability (Risk Assessment category), information protection (Information and Protection category), workforce (Awareness and Training category), and access controls (Identity Management and Access Control category). Without adequate controls in those areas, the DoD cannot ensure that:

- cybersecurity risk to operations, assets, and individuals are understood;
- personnel receive cybersecurity awareness training and perform their cybersecurity-related duties and responsibilities consistent with DoD policies and procedures; and
- security policies, processes, and procedures are in place and used to protect of information systems and assets.

The reports also identified risks in key subcategories such as establishing and communicating organizational cybersecurity policy, highlighting the risks to managing and monitoring the DoD's operational requirements. Figure 2 shows the number of reports that identify risks and findings by NIST Cybersecurity Framework category.

Figure 2. Number of Reports With Risks and Activities Identified by NIST Cybersecurity Framework Category (as of August 2020)



Note: The "other" category comprises 12 of the 23 NIST Cybersecurity Framework categories. Totals do not equal the number of reports identified because one report may cover more than one NIST Cybersecurity Framework category.

Source: The DoD OIG.

Risks by NIST Cybersecurity Framework

The 44 reports identified cybersecurity risks in all five of the NIST Cybersecurity Framework functions—Identify, Protect, Detect, Respond, and Recover. Table 2 provides the number of reports, by oversight agency, which identify risks and findings regarding each NIST Cybersecurity Framework function.

Table 2. Number of Reports 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	6	8	1	3	11	4	**33**
Protect	4	7	2	3	7	5	**28**
Detect	0	2	0	0	1	0	**3**
Respond	1	4	0	0	2	1	**8**
Recover	1	1	0	1	0	0	**3**

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

Source: The DoD OIG.

Identify Function

We determined that there were 33 reports issued—24 unclassified and 9 classified—that identified cybersecurity risks regarding the Identify function, primarily within the Asset Management, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management categories. The Identify function includes activities that develop an organizational understanding for managing cybersecurity risk to systems, people, assets, data, and capabilities. The activities enable an organization to focus and prioritize its efforts according to its risk management strategy and business needs. The reports identified risks and weaknesses regarding the Identify function—such as the establishment and communication of cybersecurity policy among DoD organizations—that limit the DoD's ability to manage cybersecurity risk. Table 3 provides the NIST Cybersecurity Framework categories under the Identify function and the desired cybersecurity outcomes.

Table 3. NIST Cybersecurity Framework Categories for the Identify Function

Category	Cybersecurity Outcomes
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 the organization's 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 decisions.
Supply Chain Risk Management	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support 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.

The following sections provide examples of risks from unclassified reports that identified risks in five categories identified under the Identify function—Asset Management, Governance, Risk Assessment, Risk Management Strategy, and Supply Chain Risk Management. For each category, we provide the number of reports that identified risks, the definition of the category, and an overview of the cybersecurity risks and examples. Specifically, we provide a summary of the report's findings, causes, effects, and status of recommendations.

Asset Management Category

We determined that there were 10 reports issued—6 unclassified and 4 classified—that identified risks regarding the Asset Management category of the NIST Cybersecurity Framework's Identify function. According to the NIST Cybersecurity Framework, the outcome of the Asset Management category is that 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 the organization's risk strategy.

The following report identified cybersecurity risks regarding the Asset Management category and the impact of the risks.

GAO Report No. GAO-20-402, "Internet Protocol Version 6: DoD Needs to Improve Transition Planning," June 1, 2020

The GAO determined that the DoD has not completed three of four OMB Internet Protocol version 6 (IPv6) transition planning requirements, including completing an inventory of existing Internet Protocol-compliant devices and technologies, developing a cost estimate and conducting a risk analysis for the transition of IPv6.[22] Furthermore, the GAO determined that the DoD had not completed most of its own required transition activities. Specifically, the DoD had completed only 6 of the 18 activities that were to be completed by March 2020.

According to the GAO, DoD officials stated that this occurred because completing an inventory of existing Internet Protocol–compliant devices and technologies would be impractical given the DoD's size and the number of Internet Protocol-compliant devices. The DoD also did not complete a cost estimate or risk analysis because the initiative was not a top priority until the DoD Chief Information Officer (CIO) released the "Internet Protocol Version 6 Implementation Direction and Guidance" memorandum in February 2019. Furthermore, DoD officials leading the IPv6 transition effort stated that the DoD had not yet completed its required activities because the original time frames that the DoD had established were unrealistic. Without an inventory, a cost estimate, or a risk analysis, the DoD significantly reduced the probability that it could have developed a realistic transition schedule.

According to NIST, having an inventory of Internet Protocol-compliant assets is crucial to IPv6 transition planning because it helps determine transition requirements and gives an agency a clear understanding of the Internet Protocol capabilities of the devices on the network. Specifically, an inventory helps determine which assets will transition to IPv6, the order in which assets will transition, the transition methods selected, and the security controls that would need to be implemented.[23]

The GAO made three recommendations concerning the transition to IPv6, including that the Secretary of Defense direct the DoD CIO to complete a DoD-wide inventory of existing Internet Protocol–compliant devices and technologies to help with

[22] Internet Protocol addresses provide a numerical description of the location of networked devices such as computers, routers, and smartphones. These numerical descriptions allow devices to be distinguished from each other over the Internet. The Internet Engineering Task Force, the principal body engaged in the development of Internet standards, developed IPv6 in the 1990s to address IPv4's limited address space, among other things. Although IPv6 has been available for over 20 years, IPv4, the older IP, is still more widely used.

[23] NIST Special Publication 800-119, "Guidelines for the Secure Deployment of IPv6," December 2010.

planning efforts and requirements development for the transition to IPv6. As of August 2020, all three recommendations remained open, and two of these three recommendations were resolved.

Asset Management Category Trends

We determined that the DoD continues to face challenges with cybersecurity issues regarding Asset Management. For example, four reports identified findings regarding how physical devices and systems within the organization are inventoried. By implementing the recommendations identified in the reports, the DoD can improve its ability to manage and identify assets to achieve organizational objectives.

Governance Category

We determined that there were 19 reports issued—12 unclassified and 7 classified—that identified risks regarding the Governance category of the NIST Cybersecurity Framework's Identify function. According to the NIST Cybersecurity Framework, the outcome of the Governance category is that the policies, procedures, and processes that are in place to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

The following two reports identified cybersecurity risks regarding the Governance category and the impact of the risks.

DoD OIG Report No. DODIG-2020-098, "Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology," June 29, 2020

The DoD OIG determined that the Joint Artificial Intelligence Center (JAIC) needed to take additional actions to develop and implement an Artificial Intelligence (AI) governance framework and standards. It also determined that since its inception in June 2018, the JAIC primarily focused on building its workforce, developing National Mission Initiatives, and adopting ethical principles for using AI.[24]

According to the DoD OIG, JAIC officials stated that this occurred because the AI governance requirements were the responsibility of the designated senior official. Furthermore, the JAIC Director was not appointed as the designated senior official until October 2019. JAIC officials further stated that the lack of a formal designation hindered their ability to develop an AI governance framework and standards because the JAIC did not have the authority to coordinate AI activities across the DoD.

[24] National Mission Initiatives are large-scale efforts to apply AI as a solution to closely related and urgent challenges the DoD may encounter.

The DoD OIG stated that developing a comprehensive governance framework during the emergence of AI will help fulfill the DoD's mission to protect the security of our Nation by developing and deploying advanced AI capabilities that ensure the United States sustains its competitive military advantage over its adversaries. The DoD OIG further stated that if the DoD does not develop an AI governance framework in a timely manner, there is an increased risk that the DoD will lose its opportunity to become a strong, technologically advanced Department, which is essential for protecting U.S. service members; safeguarding U.S. citizens; defending allies and partners; and improving the affordability, effectiveness, and speed of DoD operations.

The DoD OIG made 28 recommendations concerning AI governance and processes, including that the JAIC Director establish an AI governance framework that includes a security classification guide to ensure consistent protection of data used and produced for AI projects. As of August 2020, 25 of 28 recommendations remained open, and 18 of these 25 recommendations were resolved.[25]

Air Force Audit Agency Report No. F2020-0001-A00900, "National Air and Space Intelligence Center Security Controls," October 4, 2019

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

[25] As of August 2020, three recommendations were closed.

[26] DoD Manual 5205.07, volume 1, "DoD Special Access Program Security Manual: General Procedures," February 12, 2018.

The AFAA made two recommendations concerning standard operating procedures, including that the Commander of the National Air and Space Intelligence Center update National Air and Space Intelligence Center standard operating procedures and distribute procedures to Center personnel in accordance with DoD Manual 5205.07, volume 1, and Intelligence Community Directive 705.[27] As of August 2020, both recommendations remained open, and both of these recommendations were resolved.

Governance Category Trends

We determined that the DoD continues to face challenges with cybersecurity issues regarding governance. For example, nine reports identified findings regarding the establishment and communication of cybersecurity policy among DoD organizations. By implementing the recommendations identified in the reports, the DoD can improve its ability to develop and implement DoD policies, procedures, and processes that inform DoD management of cybersecurity risk.

Risk Assessment Category

We determined that there were 10 reports issued—7 unclassified and 3 classified—that identified risks regarding the Risk Assessment category. According to the NIST Cybersecurity Framework, the outcome of the Risk Assessment category is that the organization understands the cybersecurity risk to organizational operations, organizational assets, and individuals.

The following two reports identified risks regarding the Risk Assessment category.

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

[redacted]

27 ~~(CUI)~~ [redacted]

28 ~~(FOUO)~~ [redacted]

29 ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

GAO Report No. GAO-19-570, "Future Warfare: Army is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess The Staffing, Equipping, and Training of New Organizations," August 15, 2019

The GAO determined that the Army is establishing new cyber and electronic warfare units for multi-domain operations, but did not fully assess the risk of activating some units at an accelerated pace and is experienced staffing, equipping, and training challenges. For example, the Army activated a cyber battalion in December 2018, and as of March 2019, this unit was understaffed by more than 80 percent. Army guidance directs the Army staff to conduct assessments on new units to determine whether the Army can staff, equip, and train these organizations.

According to the GAO, this occurred because Army leadership believed the threats justified developing these units at an accelerated pace. As a result, the Army may not assess risks for units activated at an accelerated pace, and those units may be unable to effectively conduct multi-domain operations.

The GAO made three recommendations concerning assessing the staffing, equipping, and training of new organizations, including that the Secretary of the Army ensure that the Deputy Chief of Staff, G-3/5/7 assess the risk associated with staffing, equipping, and training the existing Intelligence, Cyber, Electronic Warfare, and Space unit before its incorporation into the first Multi-Domain Task Force in FY 2020. As of August 2020, one of the three recommendations remained open and unresolved.[30]

Risk Assessment Category Trends

We determined that the DoD continued to face challenges with cybersecurity issues regarding Risk Assessment. For example, five reports identified findings regarding identifying and documenting DoD operation, asset, and personnel vulnerabilities. By implementing the recommendations identified in the reports, the DoD can improve its ability to understand the cybersecurity risk to DoD operations, assets, and personnel.

[30] As of August 2020, two recommendations were closed.

Risk Management Strategy Category

We determined that there were five unclassified reports issued that identified risks regarding the Risk Management Strategy category. According to the NIST Cybersecurity Framework, the outcome of the Risk Management Strategy category is that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational decisions.

The following report identified cybersecurity risks regarding the Risk Management Strategy category and the impact of the risks.

(FOUO) [redacted]

(FOUO) [redacted]

(FOUO) [redacted]

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

(FOUO) [redacted]

[31] (FOUO) [redacted]

[32] (FOUO) [redacted]

~~(FOUO)~~ [redacted]

Risk Management Strategy Category Trends

We determined that the DoD continues to face challenges with cybersecurity issues regarding the Risk Management Strategy category. For example, all five reports had findings regarding organizational stakeholders establishing, managing, and agreeing to risk management processes. By implementing the recommendations identified in the reports, the DoD will establish priorities, constraints, risk tolerances, and assumptions that support the DoD's operational decisions.

Supply Chain Risk Management Category

We determined that there were six reports issued—four unclassified and two classified—that identified risks regarding the Supply Chain Risk Management category. According to the NIST Cybersecurity Framework, there are two outcomes of the Supply Chain Risk Management category. The first outcome is that the organization's priorities, constraints, risk tolerances, and assumptions are established and used to support decisions associated with managing supply chain risk. The second outcome is that the organization has implemented the processes to identify, assess, and manage supply chain risks.

The following report identified cybersecurity risks regarding the Supply Chain Risk Management category and the impact of the risks.

Air Force Audit Agency Report No. F2019-0005-L30000, "Flexible Information Assurance Acquisition Tool Contract Management," July 18, 2019

The AFAA determined that Air Force personnel did not purchase cryptographic and crypto-related cybersecurity products and services in accordance with Air Force guidance. Specifically, personnel did not coordinate with the acquisition authority before awarding 5 of 18 crypto-related contract actions reviewed.

[33] As of August 2020, five recommendations were closed.

The AFAA stated that this occurred for the following reasons.

- Acquisition personnel were not familiar with the functional communications security guidance requiring coordination with the Cryptologic and Cyber Systems Division as the Air Force's acquisition authority.
- Air Force Life Cycle Management Center personnel did not disseminate information about crypto-related tools throughout the Air Force.
- Cryptologic and Cyber Systems Division personnel did not establish procedures to process and coordinate the development or procurement of crypto-related products and services.
- Cryptologic and Cyber Systems Division personnel did not institute controls to identify noncompliance with requirements to coordinate the purchase of crypto-related products and services.

According to the AFAA, personnel could not provide reasonable assurance of interoperability, security, accountability, and standardization for cryptographic item purchases (valued at more than $20.9 million) without Cryptologic and Cyber Systems Division coordination.

The AFAA made three recommendations concerning the purchase of cryptographic and crypto-related cybersecurity products, including that the Assistant Secretary of the Air Force for Acquisition, Technology, and Logistics should notify acquisition personnel of the requirement to coordinate crypto-related development and procurement with the communications security acquisition authority and the availability of the Flexible Information Assurance Acquisition Tool contracts. As of August 2020, all three recommendations remained open and resolved.

Supply Chain Risk Management Category Trends

We determined that the DoD continues to face challenges with cybersecurity issues regarding Supply Chain Risk Management. For example, two of the reports identified discrepancies regarding routinely assessing suppliers and third-party partners using audits, test results, or other forms of evaluations to confirm they are meeting contractual obligations. By implementing the recommendations identified in the reports, the DoD can improve its processes that identify, assess, and manage supply chain risks and support decisions associated with managing supply chain risk.

Protect Function

We determined that there were 28 reports issued—20 unclassified and 8 classified—that identified cybersecurity risks regarding the Protect function, primarily within the Identity Management and Access Control; Awareness and Training; Data Security; and Information Protection Processes and Procedures

categories. The Protect function includes those activities that assist an organization in developing and implementing appropriate safeguards to ensure delivery of critical services. These reports identified risks and weaknesses regarding the Protect function—such as inconsistent implementation of security controls to safeguard information and lack of formal training—that limit the DoD's ability to manage cybersecurity risk. 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

Category	Cybersecurity Outcomes
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.

Source: NIST Cybersecurity Framework.

The following sections provide examples from unclassified reports that identified risks and improvements in four categories identified under the Protect function—Identity Management and Access Control; Awareness and Training; Data Security; and Information Protection Processes and Procedures. For each category, we provide the number of reports that identified risks, the definition of the category, and an overview of the cybersecurity risks and examples. Specifically, we provide a summary of the report's findings, causes, effects, and status of recommendations.

Identity Management and Access Control Category

We determined that there were 11 reports issued—9 unclassified and 2 classified—that identified risks regarding the Identity Management and Access Control category. According to the NIST Cybersecurity Framework, the outcome of the Identity Management and Access Control category is that access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

The following report identified examples of cybersecurity risks regarding the Identity Management and Access Control category and the impact of those risks.

Air Force Audit Agency Report No. F2019-0012-A00900, "Secure Facility Utilization," July 9, 2019

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

- ~~(CUI)~~ [redacted]
- ~~(CUI)~~ [redacted]

- ~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

~~(CUI)~~ [redacted]

Identity Management and Access Control Category Trends

We determined that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Identity Management and Access Control category. For example, four of the reports identified risks regarding the protection and management of physical access to assets. By implementing the recommendations identified in the reports, the DoD can improve its ability to prevent unauthorized access to DoD systems and networks.

Awareness and Training Category

We determined that there were seven reports issued—six unclassified and one classified—that identified risks regarding the Awareness and Training category. According to the NIST Cybersecurity Framework, the outcome of the Awareness and Training category is that the organization's personnel and partners are provided cybersecurity awareness education and training that is needed to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

[34] As of August 2020, five recommendations were closed.

The following report identified examples of cybersecurity risks regarding the Awareness and Training category and the impact of those risks.

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

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

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

Awareness and Training Category Trends

We determined that the DoD has made progress toward improving awareness and training, but continues to face challenges. For example, five of the reports identified risks regarding all system users being informed and trained. By implementing the recommendations identified in the reports, the DoD will enable the cybersecurity workforce to perform their duties and responsibilities.

[35] As of August 2020, three recommendations were closed.

Data Security Category

We determined that there were six reports issued—five unclassified and one classified—that identified risks regarding the Data Security category. According to the NIST Cybersecurity Framework, the outcome of the Data Security category is that information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

The following report identified examples of cybersecurity risks regarding the Information Protection Processes and Procedures category and the impact of those risks.

Air Force Audit Agency Report No. F2020-0008-O10000, "Networked Data Protection," February 24, 2020

~~(CUI)~~ The AFAA determined that Air Force personnel did not protect data on SharePoint sites, process PII breach incidents as required, or comply with DoD PII mandates for information technology systems. [redacted]

~~(CUI)~~ [redacted] Furthermore, the Office of the Secretary of the Air Force, Deputy CIO did not require organizational SharePoint site collection administrators to perform periodic PII scans and report all findings to their designated privacy manager. [redacted]

The AFAA made five recommendations concerning the protection of networked data, including that the Deputy CIO of the Office of the Secretary of the Air Force reinforce the requirements to Air Force personnel to implement data-at-rest encryption controls and perform Privacy Impact Assessments when storing personnel information on SharePoint sites. As of August 2020, three of five recommendations remained open and resolved.[36]

[36] As of August 2020, two recommendations were closed.

Data Security Category Trends

We determined that the DoD continues to face challenges with cybersecurity issues regarding the Data Security category. For example, four of the reports identified risks regarding the protection of data-at-rest. By implementing the recommendations identified in the reports, the DoD can improve how it protects the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures Category

We determined that there were 11 reports issued—7 unclassified and 4 classified—that identified risks regarding the Information Protection Processes and Procedures category. According to the NIST Cybersecurity Framework, the outcome of the Information Protection Processes and Procedures category is that security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.

The following reports identified examples of cybersecurity risks regarding the Information Protection Processes and Procedures category and the impact of those risks.

Air Force Audit Agency Report No. F2019-0013-A00900, "Space Deconfliction System," July 17, 2019

The AFAA determined that Strategic Warning and Surveillance Systems personnel did not properly implement cybersecurity measures and document system security parameters in accordance with DoD guidance and maintained outdated cybersecurity documentation such as an outdated Plan of Action and Milestones.

Specifically, the program manager sustained two of three system strings on expired authorization decisions and maintained outdated or incomplete cybersecurity documentation.[37] For example, program personnel had not updated Plan of Action and Milestones documents since October 2017.

According to the AFAA, this occurred because program personnel did not: (1) properly manage security authorization documents by aligning applicable guidance or following up on required actions; (2) establish a process to maintain consistency across multiple security authorization packages; and (3) ensure that all program personnel had access to required systems. The AFAA stated that implementing cybersecurity control measures minimizes potential loss of confidentiality, integrity, and availability of data and information systems.

[37] The Space Deconfliction System is segregated into three standalone iterations "strings" of the system that operate at different classification levels. Each string requires an independent security authorization package with an authorization decision from respective authorizing officials.

Furthermore, strong cybersecurity reduces potential for exploitation of vulnerabilities leading to security breaches, impacts to the space laser avoidance mission, and potential damage to national space assets.

The AFAA made two recommendations concerning cybersecurity measures and system security parameters, including that the Chief of the Air Force Life Cycle Management Center's Strategic Warning and Surveillance Systems Division ensure personnel responsible for developing and updating security authorization packages have access to all necessary systems and suites to monitor, evaluate, and respond. As of August 2020, both recommendations were closed.

GAO Report No. GAO-19-457, "Information Technology: DoD Needs to Fully Implement Program for Piloting Open Source Software," September 10, 2019

The GAO determined that the DoD has not fully implemented an open source software pilot program and related OMB requirements as mandated by the National Defense Authorization Act for Fiscal Year 2018. Specifically, the GAO determined that the DoD has not fully implemented OMB Memorandum M-16-21 requirements to implement a pilot program.[38] In addition, the GAO determined that DoD has not implemented other OMB memorandum requirements for issuing policy and partially implemented requirements for conducting analyses of software solutions, securing data rights and inventory code, and facilitating the open source community.

According to the GAO, this occurred because the DoD had not implemented the requirement to develop a consistent measure to gauge the performance of the DoD's pilot program due to a lack of consensus in the DoD about what data should be collected. The DoD acknowledged that it did not have a policy that addressed the OMB memorandum's requirement. Until the DoD fully implements the open source software pilot program mandated in the National Defense Authorization Act for Fiscal Year 2018, including the requirements of OMB Memorandum M-16-21, the DoD will likely miss opportunities to achieve related cost savings and efficiencies. Furthermore, the DoD will not be effectively positioned to ensure management oversight and implementation of the pilot program.

The GAO made four recommendations concerning piloting open source software, including that the Secretary of Defense ensure that the DoD establishes milestones for completing the requirements of OMB Memorandum M-16-21 for securing data rights and conducting an inventory. As of August 2020, two of four recommendations remained opened and unresolved.[39]

[38] OMB Memorandum M-16-21, "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation Through Reusable and Open Source Software," August 8, 2016.

[39] As of August 2020, two recommendations were closed.

Information Protection Processes and Procedures Category Trends

We determined that the DoD has made progress toward improving information protection processes and procedures, but continues to face challenges. For example, three of the reports identified risks regarding the establishment and management of response and recovery plans. By implementing the recommendations identified in the reports, the DoD can improve its ability to maintain security policies, processes, and procedures used to protect DoD information systems and assets.

Detect Function

We determined that there were three unclassified reports issued that identified risks regarding the Detect function, within the Anomalies and Events and Security Continuous Monitoring categories. 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 regarding the Detect function—such as contractors not conducting network scans for viruses and vulnerabilities—that limits the DoD's ability to manage cybersecurity risk. 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

Category	Cybersecurity Outcomes
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.

The following section provides examples from the unclassified reports that identified risks in categories identified under the Detect function—Anomalies and Events and Security Continuous Monitoring. For each category, we provide the number of reports that identified risks, the definition of the category, and an overview of the cybersecurity risks and examples. Specifically, we provide a summary of the report's findings, causes, effects, and status of recommendations.

Anomalies and Events

We determined that there was one unclassified report issued that identified risks regarding the Anomalies and Events category. According to the NIST Cybersecurity Framework, the outcome of the Anomalies and Events category is an anomalous activity that is detected and the potential impact of its events understood.[40]

The following report identified cybersecurity risks regarding the Anomalies and Events category and the impact of those risks.

DoD Office of Inspector General Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019

The DoD OIG determined that DoD contractors did not consistently implement security controls in accordance with Federal and DoD requirements for safeguarding Defense CUI. For example, DoD Component contracting offices did not establish processes to:

- verify that contract offerors' networks and systems that process, store, and transmit CUI met the NIST security requirements before contract award;
- notify contractors of the specific CUI category regarding the contract requirements;
- determine whether contractors accessed, maintained, or developed CUI to meet contractual requirements;
- properly mark documents that contained CUI; and
- verify that contractors implemented minimum security controls required by NIST guidance.

The DoD OIG stated that the DoD did not know the amount of DoD CUI managed by contractors and did not have accurate information to determine whether contractors are protecting CUI from unauthorized access and disclosure. Without knowing which contractors maintain CUI on their networks and systems and taking actions to validate that contractors protect and secure DoD information, the DoD is at greater risk of its CUI being compromised by cyber attacks from malicious actors who target DoD contractors and steal information regarding some of the Nation's most valuable advanced Defense technologies. Preventing cyber attacks against DoD contractor networks and systems requires implementation of system security controls that reduce the vulnerabilities that malicious actors use to compromise DoD critical national security information.

[40] Anomalies within organizational information systems include large file transfers, long-time persistent connections, unusual protocols and ports in use, and attempted communications with suspected malicious external addresses.

The DoD OIG made 45 recommendations concerning the protection of DoD CUI, including actions for DoD officials to revise policy to include language that required DoD Component contracting offices and requiring activities to assess contractor compliance with NIST requirements. As of August 2020, 17 of 45 recommendations remained open, and 12 of these 17 recommendations were resolved.[41]

Anomalies and Events Category Trends

We identified only one report with findings regarding the Anomalies and Events category of the NIST Cybersecurity Framework. Therefore, we did not identify trends for this category in the Detect function.

Security Continuous Monitoring

We determined that there were two unclassified reports issued that identified risks regarding the Security Continuous Monitoring category. According to the NIST Cybersecurity Framework, the outcome of the Security Continuous Monitoring category is that information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

The following report identified cybersecurity risks regarding the Security Continuous Monitoring category and the impact of those risks.

Air Force Audit Agency Report No. F2020-0003-O10000, "Risk Management Framework: Weather Systems," December 3, 2019

The AFAA determined that although Air Force personnel complied with RMF guidance when establishing weather system authorization boundaries, they did not perform configuration management in accordance with RMF requirements.[42] Furthermore, Air Force personnel were unable to demonstrate that they had current and accurate software baseline data and therefore were not in compliance with the RMF configuration management requirements. The AFAA determined that this occurred because Air Force personnel did not have an automated tool in place to identify systems that were not compliant with approved baseline configurations.

The AFAA stated that configuration management helps detect unauthorized hardware, software, or firmware changes that could introduce vulnerabilities to the network.

[41] As of August 2020, 28 recommendations were closed. Requiring activities are DoD Components that identify required contracted services to accomplish their mission.

[42] Configuration management is a process for establishing an information system component's (such as servers or operating systems) performance, function, and physical attributes throughout its life cycle. Configuration management ensures components and their settings are known and tracked, and all changes are recorded.

The AFAA made two recommendations concerning compliance with the RMF requirements, including actions for the Air Force Deputy Chief of Staff for Operations to direct the Director of Weather to obtain an automated tool that will enable the identification of weather systems that are not in compliance with approved baseline configurations. As of August 2020, both recommendations remained open and resolved.

Security Continuous Monitoring Category Trends

We determined that the DoD continues to face significant challenges in managing cybersecurity risks associated with the Security and Continuous Monitoring Category. For example, both reports identified risks regarding network monitoring to detect potential cybersecurity events. By implementing the recommendations identified in the reports, the DoD can monitor information systems and assets to identify cybersecurity events and verify the effectiveness of protective measures.

Respond Function

We determined that there were eight reports issued—four unclassified and four classified—that identified cybersecurity risks or activities regarding the Respond function, primarily within the Communications category. The Respond function includes those activities that demonstrate the development and implementation of appropriate activities in order to take action regarding a detected cybersecurity incident. These reports identified risks or activities regarding the Respond function—such as the sharing of information regarding security incidents and compromises with the Air Force SAP Oversight Review Board. These risks limit the DoD's ability to manage cybersecurity risk. 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

Category	Cybersecurity Outcomes
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, such as 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/response activities.

Source: NIST Cybersecurity Framework.

The following section provides an example from an unclassified report that identified activities in the Communications category under the Respond function. For the category, we provide the number of reports that identified risks or activities, the definition of the category, and an overview of the cybersecurity risks and examples. Specifically, we provide a summary of the report's findings, causes, effects, and status of recommendation.

Communications Category

We determined that there were two unclassified reports issued that identified risks or activities regarding the Communications Category. According to the NIST Cybersecurity Framework, the outcome of the Communications category is that response activities are coordinated with internal and external stakeholders.

The following report identified how Communication activities affected DoD operations and the impact of those activities.

Office of the Inspector General of the Intelligence Community Report No. AUD-2019-005-U, "Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 19, 2019

The Intelligence Community OIG determined that the sharing of cyber threat indicators and defensive measures has improved over the 2-year period assessed, and efforts are underway to expand accessibility to information.[43] For example, in April 2017, the Intelligence Community deployed the Intelligence Community Analysis and Signature Tool to increase sharing of cybersecurity threat intelligence at the Top Secret level. Additionally, the Intelligence Community OIG found that various websites increased the amount of shared cybersecurity information in the 2-year period. For example, the Intelligence Community Security Coordination Center maintained a website on the Top Secret network containing various reports on the security and vulnerabilities of information technology infrastructure. According to the Intelligence Community OIG, the availability of information for defending systems and networks against cyber attacks improved as the sharing of cyber threat indicators and defensive measures improved. The Intelligence Community OIG did not make any recommendations in this report.

[43] According to section 1501(6), title 6, United States Code, cyber threat indicators include threat-related information, such as methods of defeating or causing users to unwittingly enable the defeat of security controls and methods of exploiting cybersecurity vulnerabilities. According to section 1501(7)(A), defensive measures include an action, device, procedure, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or vulnerability. The Offices of the Inspectors General of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and Treasury, and the Intelligence Community assessed the implementation of the Statute for the calendar year 2017 and 2018 for their respective entities implementation of Public Law 114-113, "Consolidated Appropriations Act," 2016. The Office of the Inspector General of the Intelligence Community compiled the results in the report.

Communications Category Trends

We determined that although the DoD has made improvements regarding the Communications category, significant challenges still exist in managing cybersecurity risks. For example, one of the reports identified risks regarding information sharing of security incidents and compromises with Air Force officials. By implementing the recommendations identified in the reports, the DoD should improve its ability to coordinate response activities with internal and external stakeholders.

Recover Function

We determined that there were three reports issued—two unclassified and one classified—that identified cybersecurity risks regarding the Recover function, primarily within the Recovery Planning and Improvements categories. The Recover function includes activities that support timely recovery of normal operations to reduce the impact from a cybersecurity incident. These reports identified risks and weaknesses regarding the Recover function—such as not having the capability to recover from catastrophic emergencies—that limit the DoD's ability to manage cybersecurity risk. 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

Category	Cybersecurity Outcomes
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, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, and vendors.

Source: NIST Cybersecurity Framework.

The following sections provide examples of unclassified reports that identified risks in two categories identified under the Recover function—Recovery Planning and Improvements. For each category, we provide the number of reports that identified risks or activities, the definition of the category, and an overview of the cybersecurity risks and examples. Specifically, we provide a summary of the report's findings, causes, effects, and the status of recommendation.

Recovery Planning Category

We determined that there were two reports—one unclassified and one classified—issued that identified risks regarding the Recovery Planning category. According to the NIST Cybersecurity Framework, the outcome of the Recovery Planning category is that the execution of processes and procedures ensure restoration of systems or assets affected by cybersecurity incidents.

The following report identified cybersecurity risks regarding the Recovery Planning category and the impact of those risks.

DoD OIG Report No. DODIG-2019-116, "Audit of Contingency Planning for DoD Information Systems," August 21, 2019

The DoD OIG determined that DoD Components did not consistently develop and test information system contingency plans (ISCPs) to recover national security systems (NSS) and data after emergencies, system failures, or disasters, in accordance with DoD and Federal guidance. Specifically, the DoD OIG found that the system owners:

- developed and tested ISCPs for only 2 of the 15 systems in accordance with minimum ISCP requirements;
- developed ISCPs for 9 of the 15 systems, but the ISCPs did not include all minimum ISCP requirements; and
- did not develop or test ISCPs for 4 of the 15 systems.

~~(FOUO)~~ According to the DoD OIG, this occurred because the DoD CIO, and the DoD Component heads and their respective CIOs, did not prioritize and ensure that ISCPs were consistently developed and tested for NSS as required by DoD and Federal guidance. For example, the DoD OIG found that the DoD CIO did not have a process or controls in place to ensure that system owners developed and maintained ISCPs as required. In addition, a DoD CIO official stated that the DoD CIO did not perform inspections or have authority to provide oversight over the DoD Components. [redacted]

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

Recovery Planning Category Trends

We determined that the DoD continues to face significant challenges regarding the Recovery Planning category. For example, one of the reports identified risks regarding the execution of a recovery plan during or after a cybersecurity incident. By implementing the recommendations identified in the report, the DoD should improve its ability to execute recovery processes.

Improvements Category

We determined that there was one unclassified report issued that identified risks regarding the Improvements category. According to the NIST Cybersecurity Framework Improvements Category, recovery planning and processes are improved by incorporating lessons learned into future activities.

The following report identified cybersecurity risks regarding the Improvements category and the impact of those risks.

~~**(FOUO)**~~ [redacted]

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

[44] As of August 2020, two recommendations were closed.

[45] ~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

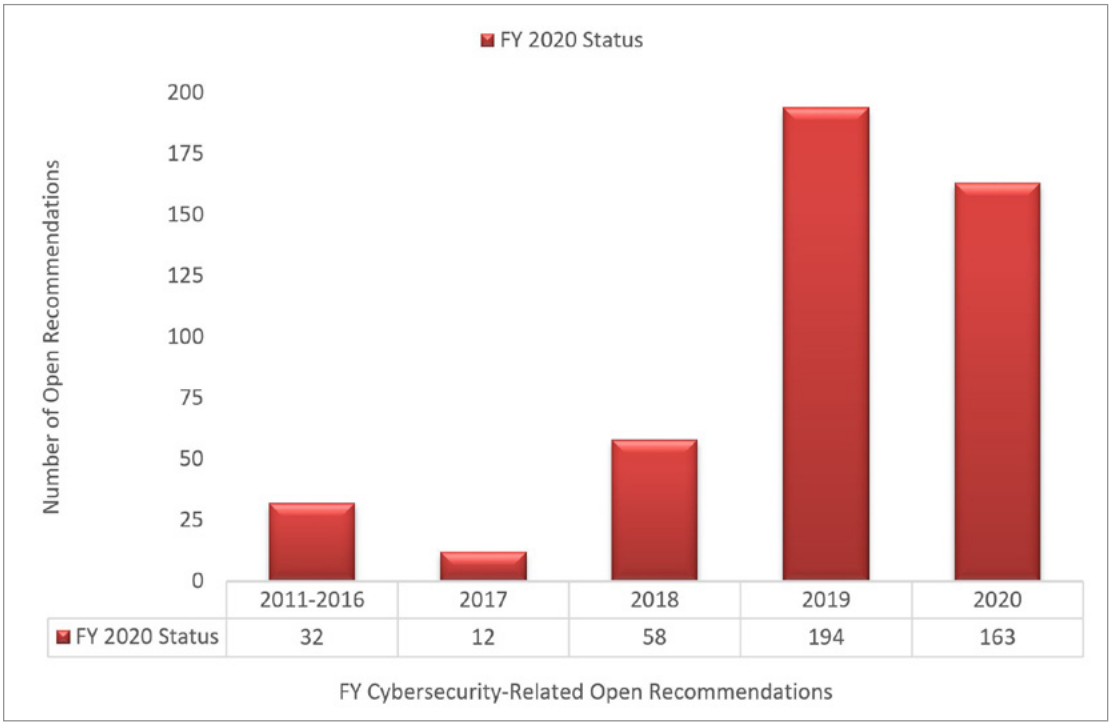
Improvements Category Trends

We determined that the DoD continues to face significant challenges regarding the Improvements category. For example, one of the reports identified risks regarding the incorporation of lessons learned into recovery plans. By implementing the recommendations identified in the report, the DoD should improve its recovery planning processes.

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. We determined that as of August 2020, the DoD needed to take action to close 459 open DoD cybersecurity-related recommendations—415 unclassified and 44 classified—from reports dating as far back as FY 2011. The DoD OIG, GAO, and 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 Recommendations by Fiscal Year of Report



Note: The FY 2019 and FY 2020 recommendations were recently issued and, therefore, DoD management may not have had sufficient time to implement all necessary actions for closure.

Source: The DoD OIG.

The DoD OIG, GAO, and the other DoD oversight organizations made 32 cybersecurity-related recommendations before FY 2017 (the oldest was made in FY 2011) that remained open as of August 2020. Of the 32 recommendations:

- the GAO made 11 recommendations to the Secretary of Defense to clarify roles and responsibilities for defense support of civil authorities, strengthen governance and management, improve roles and address challenges in exercises, and improve application inventories;
- the DoD OIG made 16 recommendations to the Under Secretary of Defense for Personnel and Readiness, the Deputy Chief Financial Officer, the DoD CIO, the Army, the Navy, and the Defense Logistics Agency, regarding physical access control systems, data loss prevention, controls and audit trails for information system processes, cloud computing strategies, and information system configuration;
- the Army made one recommendation to Critical Infrastructure Risk Management program personnel regarding the verification of task-critical asset information in the Strategic Mission Assurance Data System for accuracy and completeness; and

- the Air Force made four recommendations to the Deputy Chief of Staff, Manpower, Personnel, and Services, the Assistant Secretary of the Air Force (Financial Management and Comptroller), and the Commander of Air Force Space Command regarding access controls, contingency planning, and audit log storage capabilities; one of the four has remained open since FY 2011.

Recommendation Status for Reports and Notices of Findings and Recommendations Issued From July 1, 2019, Through June 30, 2020

The DoD OIG, GAO, and other DoD oversight organizations made 327 cybersecurity-related recommendations to the DoD in 44 reports—33 unclassified and 11 classified—issued from July 1, 2019, through June 30, 2020. Of the 327 DoD recommendations, 215 remained opened as of August 2020, with the majority of open recommendations regarding the Identify and Protect functions. As of August 2020, DoD management had agreed with 150 of the 215 open cybersecurity-related recommendations, however, 65 recommendations still remained unresolved. The unresolved DoD recommendations consisted of:

- 28 recommendations to which management did not provide a response;
- 17 recommendations with which management partially agreed;
- 12 recommendations for which management provided actions that partially addressed the identified issues; and
- 8 recommendations with which management disagreed.

For example, the DoD partially agreed with a recommendation made in Report No. DODIG-2020-098, "Audit of Governance and Protection of Department of Defense Artificial Intelligence Data and Technology." The DoD OIG recommended that the Director of the JAIC establish an AI governance framework that includes a security classification guide to ensure consistent protection of data used and produced for AI projects. The DoD CIO, responding for the JAIC Director, partially agreed, stating that the DoD CIO and the JAIC agree that comprehensive AI security guidance is needed. However, the DoD CIO stated that when the JAIC uses data from other organizations, the JAIC will use that organization's classification guidance unless the data are explicitly modified. In response, the DoD OIG stated that the DoD CIO's plan to develop a security classification guide that will apply only to AI data that the JAIC produces or explicitly modifies did not meet the intent of the recommendation. Therefore, the DoD OIG determined this recommendation was unresolved at the time the report was issued. As of August 2020, this recommendation remained open.

The DoD has numerous open recommendations that have remained unaddressed, which date as far back as FY 2011. This open recommendation from FY 2011 is from the AFAA directed toward the Air Force Space Command Commander to direct the 24th Air Force Commander to acquire sufficient storage capability for a Network Operations Security Center to retain audit logs.

In addition to the recommendations made in audits and evaluations performed by the DoD OIG, GAO, and other DoD oversight organizations, the DoD also receives recommendations for improvements as part of the ongoing efforts to audit the DoD financial statements. These recommendations are provided to the DoD in what is referred to as a Notice of Findings and Recommendations (NFRs).

As of July 1, 2020, the DoD had 1,710 open information technology NFRs as a result of the FY 2019 and FY 2020 financial statement audits and attestations conducted by independent public accounting firms (auditors) and the DoD OIG.[46] We determined that the information technology NFRs identified weaknesses related to the NIST Cybersecurity Framework.

NFRs are the mechanism that auditors use to communicate problems they identified during the audit. Similar to how DoD management agrees or disagrees with recommendations in a performance audit, the audited entity in a financial statement audit either agrees or disagrees with the NFR. However, the NFR comment process is slightly different from the performance audit recommendation comment process in that the entity does not comment on each NFR recommendation, but instead comments on the problem and NFR as a whole.

We selected a random sample of 44 of the 1,710 open information technology NFRs for review. According to "A Publication of the Inspectors General of the United States," a sample size should be 44 if the total population is between 501 and 2000.[47] As part of the review process we categorized the 44 NFRs based on the NIST Cybersecurity Framework as follows:

- 14 included risks regarding the Identity Management and Access Control category (Protect function);
- 7 included risks regarding the Information Protection Processes and Procedures category (Protect function);
- 5 included risks regarding the Asset Management category (Identify function);
- 5 included risks regarding the Governance category (Identify function);

[46] Auditors continued to issue NFRs past October 2020. Therefore, the number of open information technology NFRs does not reflect all the NFRs issued as a result of the FY 2020 financial statement audits.

[47] A Publication of the Inspectors General of the United States, The Journal of Public Inquiry, Fall/Winter 2012-2013.

- 4 included risks regarding the Supply Chain Risk Management category (Identify function);
- 4 included risks regarding the Detection Processes category (Detect function);
- 2 included risks regarding the Security Continuous Monitoring category (Detect function);
- 1 included risks regarding the Data Security category (Protect function);
- 1 included risks regarding the Protective Technology category (Protect function); and
- 1 included risks regarding the Anomalies and Events category (Detect function).

The following sections provide examples from the 44 NFRs that identified weaknesses regarding the (1) Identity Management and Access Control and (2) Information Protection Processes and Procedures categories under the Protect function. For each information technology NFR example, we provide a summary of the findings, cause, effect, recommendations, and status of recommendation.

Identity Management and Access Control (Protect Function)

We determined that 14 of the 44 NFRs we reviewed identified weaknesses regarding the Identity Management and Access Control category. According to the NIST Cybersecurity Framework, the outcome of the Identity Management and Access Control category is that access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. Specifically, 8 of the 14 NFRs included risks regarding the implementation least privilege.[48]

For example, the auditors determined that security administrators in Navy Enterprise Resource Planning system had the ability to submit, authorize, and modify their access. This occurred because systematic controls were not configured in Navy Enterprise Resource Planning system to prevent security administrators from being able to submit and approve access requests that they submitted. With the ability to authorize and modify access on their own, security administrators could have an inappropriate level of privileges in the system such as the ability to input and approve business transactions.

[48] According to NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013, Revision 4, least privilege allows only authorized accesses for users (or processes acting on behalf of users) that is necessary to accomplish assigned tasks in accordance with the organizational missions and business functions.

The auditors recommended that Navy Enterprise Resource Planning management configure the Navy Enterprise Resource Planning application to prevent security administrators, or any users, from having the ability to add, modify, or remove their own access in the application. As of July 1, 2020, the recommendation remained open.

Information Protection Processes and Procedures (Protect Function)

We determined that 7 of the 44 NFRs we reviewed identified weaknesses regarding the Information Protection Processes and Procedures category. According to the NIST Cybersecurity Framework, the outcome of the Information Protection Processes and Procedures category is that security policies, processes, and procedures are maintained and used to manage protection of information systems and assets. Specifically six of the seven NFRs identified risks regarding configuration management.[49]

For example, the auditors determined that developers had write access permissions to production files for a Defense Finance and Accounting Services Transaction Interface Module.[50] This occurred because management did not update the access control policies to address access restrictions for write permissions. If access restrictions are not in place for a system's production environment, there is an increased risk that unauthorized modifications may be implemented, which adversely impact system functionality and security.

The auditors recommended that management update access control policies to identify access restrictions for write permissions for the module. In addition, the auditors recommended that management review the groups with write permissions to production files and verify that developers from the configuration management team did not have inappropriate access. As of July 1, 2020, the recommendations remained open.

Trends From Financial Statement Information Technology NFRs

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. In addition, DoD Components did not own and operate all of the information technology systems that they use to process their financial transactions.

[49] According to NIST Special Publication 800-53 Revision 4, configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

[50] Permitted actions are enforced by the information system and include, for example, read, write, execute, append, and delete privileges.

To address the large number of open information technology NFRs, the DoD is developing a business plan that will outline the number of systems that impact financial reporting that it plans to retire, resulting in a reduced footprint of systems that impact financial reporting. This plan includes a decrease of 51 legacy information technology systems between FYs 2019 and 2023.[51]

The lack of effective 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 the information technology NFRs will better enable the DoD to improve its overall reliance on the accuracy and completeness of financial-related data. 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 ensure that it implements effective risk management practices to reduce cybersecurity risks affecting the DoD Information Network and all business and military operations.

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

Appendix A

Scope and Methodology

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

This report summarizes unclassified reports issued by the DoD OIG, GAO, and the other DoD oversight organizations from July 1, 2019, through June 30, 2020. To prepare this summary, we coordinated with members of the DoD audit community, the Intelligence Community agencies, and the GAO to obtain unclassified reports in this summary and classified reports (up to SECRET) in Appendix E. We reviewed the findings, recommendations, and statements made in each report and categorized the reports based on the 5 NIST Cybersecurity Framework functions and 23 categories to determine whether they related to the NIST Cybersecurity Framework. We did not review supporting documentation for any of the reports. Additionally, because the summarized reports contain recommendations regarding the identified cybersecurity risks, this summary report does not contain additional recommendations.

This report also summarizes information technology NFRs for the DoD. To prepare this summary, we coordinated with the DoD OIG Quantitative Methods Division to develop a random sample of information technology NFRs. As of July 1, 2020, the DoD had 1,710 open information technology NFRs. Based on this universe of open information technology NFRs, we selected a random sample of 44 NFRs and provided a summary of the NFRs' findings as they pertain to the NIST Cybersecurity Framework.[52]

Use of Computer-Processed Data

We obtained the total universe of open information technology NFRs from the Office of the Deputy Chief Financial Officer NFR Database as of July 1, 2020. The NFR Database reports real-time information on the progress of the DoD financial statement audits. In particular, the database contains all NFRs, corrective action plans, status of actions taken, and the status of the NFR from each stand-alone financial statement audit, the DoD Consolidated Audit, and service provider examinations. We determined that the total number of open information technology NFRs obtained from the NFR Database was sufficient and reliable to support the NFRs' findings as they pertain to the NIST Cybersecurity Framework.

[52] The sample size is based on "A Publication of the Inspectors General of the United States," by Dr. Kandasamy Selvavel and James Hartman Jr., Fall/Winter 2012-2013, publication page 46, Figure 3, Population Size (N) 501-2000.

Prior Coverage

During the last 5 years, the DoD OIG issued five reports summarizing 140 DoD cybersecurity-related reports—123 unclassified and 17 classified—and five unclassified 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/reports.html/.

DoD OIG

Report No. DODIG-2020-089, "Summary of Reports and Testimonies Regarding DoD Cybersecurity From July 1, 2018, Through June 30, 2019," June 11, 2020 (Report is FOUO)

> The DoD OIG identified 46 DoD cybersecurity-related reports—33 unclassified and 13 classified—and 3 testimonies provided to Congress by the DoD OIG, GAO, and other DoD oversight organizations from July 1, 2018, through June 30, 2020. The DoD OIG 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 prior summary reports. Those corrective actions mitigated or remediated risks and weaknesses to DoD systems and networks. However, despite numerous improvements made by the DoD over the past year, the DoD continues to face significant challenges in managing cybersecurity risks to its systems and networks. As of September 30, 2019, the DoD had 330 cybersecurity-related recommendations that remained open, dating back to 2011.

Report No. DODIG-2019-044, "Summary of Reports Issued Regarding DoD 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 between July 1, 2017, through June 30, 2018, regarding 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 1 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 the 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 1 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 the 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.

Appendix B

Unclassified and Classified Reports Regarding DoD Cybersecurity

GAO

1. Report No. GAO-20-402, "Internet Protocol Version 6: DoD Needs to Improve Transition Planning," June 1, 2020
2. Report No. GAO-20-241, "Cybersecurity: DoD Needs to Take Decisive Actions to Improve Cyber Hygiene," April 13, 2020
3. Report No. GAO-20-279, "Data Center Optimization: Agencies Report Progress, but Oversight and Cybersecurity Risks Need to Be Addressed," March 5, 2020
4. Report No. GAO-20-272, "Federally Funded Research and Development Centers: Improved Oversight and Evaluation Needed for DoD's Data Access Pilot Program," March 6, 2020
5. Report No. GAO-20-299, "Critical Infrastructure Protection: Additional Actions Needed to Identify Framework Adoption and Resulting Improvements," February 25, 2020
6. Report No. GAO-20-129, "Information Technology: Agencies Need to Fully Implement Key Workforce Planning Activities," October 30, 2019
7. Report No. GAO-19-457, "Information Technology: DoD Needs to Fully Implement Program for Piloting Open Source Software," September 10, 2019
8. Report No. GAO-19-499C, "Military Readiness: Readiness Improved in the Ground and Cyber Domains but Declined in the Sea, Air, and Space Domains from Fiscal Year 2017 to Fiscal Year 2018," August 30, 2019 (Report is SECRET)
9. Report No. GAO-19-570, "Future Warfare: Army is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations," August 15, 2019

DoD OIG

10. Report No. DODIG-2020-098, "Audit of Governance and Protection of DoD Artificial Intelligence Data and Technology," June 29, 2020 (Report is FOUO)
11. Report No. DODIG-2019-116, "Audit of Contingency Planning for DoD Information Systems," August 21, 2019 (Report is FOUO)

12. Report No. DODIG-2019-106, "Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items," July 26, 2019 (Report is SECRET//NOFORN)
13. Report No. DODIG-2019-105, "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems," July 23, 2019 (Report is FOUO)
14. Report No. DODIG-2019-127, "Audit of Access Controls in the Defense Logistics Agency's Commercial and Government Entity Code Program," September 30, 2019 (Report is FOUO//Law Enforcement Sensitive)
15. Report No. DODIG-2020-025, "Evaluation of the Algorithmic Warfare Cross-Functional Team (Project MAVEN)," November 8, 2019 (Report is SECRET//NOFORN)
16. Report No. DODIG-2020-068, "Audit of Security Controls Over the Department of Defense's Global Command and Control System-Joint Information Technology System" March 18, 2020 (Report is SECRET)
17. Report No. DODIG-2020-067, "Followup Audit on Corrective Actions Taken by DoD Components in Response to DoD Cyber Red Team-Identified Vulnerabilities and Additional Challenges Facing DoD Cyber Red Team Missions," March 13, 2020 (Report is SECRET//NOFORN)
18. Report No. DODIG-2020-066, "Audit of the Department of Defense Supply Chain Risk Management Program for Nuclear Command, Control, and Communications Systems," March 2, 2020 (Report is SECRET)

Army Audit Agency

19. ~~(FOUO)~~ [redacted]
20. ~~(FOUO)~~ [redacted]
21. ~~(FOUO)~~ [redacted]

Naval Audit Service

22. ~~(FOUO)~~ [redacted]
23. ~~(FOUO)~~ [redacted]
24. ~~(FOUO)~~ [redacted]

Air Force Audit Agency

25. Report No. F2020-0010-O10000, "Industrial Control Systems Access Controls," April 17, 2020
26. Report No. F2020-0008-O10000, "Networked Data Protection," February 24, 2020 (Report is FOUO)
27. Report No. F2020-0005-O10000, "Risk Management Framework Resourcing and Implementation," December 23, 2019
28. Report No. F2020-0004-O10000, "Agreed-Upon Procedures: Project Management Resource Tool - Test of Design and Effectiveness," December 10, 2019
29. Report No. F2020-0003-O10000, "Risk Management Framework - Weather Systems," December 3, 2019
30. Report No. F2020-0002-O10000, "Cybersecurity Workforce Improvement Program," October 25, 2019
31. Report No. F2020-0001-O10000, "Information Technology Hardware Asset Purchasing," October 17, 2019
32. Report No. F2020-0001-A00900, "National Air and Space Intelligence Center Security Controls," October 4, 2019 (Report is FOUO)
33. Report No. F2019-0016-A00900, "Special Access Program Justification Review," September 25, 2019
34. Report No. F2019-0007-O10000, "Risk Management Framework Tests and Assessments," August 13, 2019
35. Report No. F2019-0014-A00900, "Information Technology Parts," July 30, 2019 (Report is FOUO)
36. Report No. F2019-0005-L30000, "Flexible Information Assurance Acquisition Tool Contract Management," July 18, 2019
37. Report No. F2019-0013-A00900, "Space Deconfliction System," July 17, 2019
38. Report No. F2019-0012-A00900, "Secure Facility Utilization," July 9, 2019 (Report is FOUO)

Other DoD Agencies

39. Defense Intelligence Agency OIG Report No. 2019-1003, "Controls for Managing Network and Facility Access for Out-Processing Personnel," June 12, 2020 (Report is SECRET//NOFORN)
40. Office of the Inspector General of the Intelligence Community Report No. AUD-2019-005-U, "Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 19, 2019

41. (U//FOUO) [redacted]

42. NSA OIG Report No. IN-18-0009, "Inspection of NSA Central Security Service Representative and Cryptologic Services Group Representative to U.S. Pacific Command," August 16, 2019 (Report is FOUO)

43. NSA OIG Report No. JT-18-0003, "Joint IG Inspection Report – NSA Hawaii," August 26, 2019 (Report is SECRET//NOFORN)

44. NSA OIG Report No. IN-019-0001, "Inspection of NSA Cryptologic Representative U.S. Transportation Command," December 19, 2019 (Report is FOUO)

Appendix C

Reports Identifying Risks by NIST Cybersecurity Framework Category

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																							
	Identify						Protect						Detect			Respond					Recover			
	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	Recovery Planning	Improvements	Communications
GAO																								
GAO-20-402	x																							
GAO-20-241			x					x																
GAO-20-279	x																							
GAO-20-272							x																	
GAO-20-299			x			x																		
GAO-20-129								x																
GAO-19-457			x							x														
GAO-19-570				x																				

Reports Identifying Risks by NIST Cybersecurity Framework Category (cont'd)

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																					
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
DoD OIG																							
DODIG-2020-098			x				x		x			x		x									
DODIG-2019-127			x				x	x	x														
DODIG-2019-116										x											x		
DODIG-2019-105			x	x		x	x			x		x	x						x				

Reports Identifying Risks by NIST Cybersecurity Framework Category (cont'd)

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																		
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Army Audit Agency																							
~~(FOUO)~~ [redacted]	[redacted]																						
~~(FOUO)~~ [redacted]																							
~~(FOUO)~~ [redacted]																							
Naval Audit Service																							
~~(FOUO)~~ [redacted]	[redacted]																						
~~(FOUO)~~ [redacted]																							
~~(FOUO)~~ [redacted]																							

~~(FOUO)~~

Reports Identifying Risks by NIST Cybersecurity Framework Category (cont'd)

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																						
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Air Force Audit Agency																							
F2020-0010-O10000	x			x																			
F2020-0008-O10000									x														
F2020-0005-O10000					x																		
F2020-0004-O10000							x																
F2020-0003-O10000									x	x				x									
F2020-0002-O10000	x																						
F2020-0001-O10000			x																	x			
F2020-0001-A00900	x		x				x																
F2019-0016-A00900				x													x						
F2019-0007-O10000					x																		
F2019-0014-A00900		x				x																	

Reports Identifying Risks by NIST Cybersecurity Framework Category (cont'd)

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																						
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Air Force Audit Agency (cont'd)																							
F2019-0005-L30000						x		x															
F2019-0013-A00900				x						x													
F2019-0012-A00900			x				x																
Other DoD Organizations																							
AUD-2019-005-U																	x						

Reports Identifying Risks by NIST Cybersecurity Framework Category (cont'd)

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																					
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Totals																							
Unclassified Reports Subtotal	6	3	12	7	5	4	9	6	5	7	0	2	1	2	0	0	2	0	1	1	1	1	0
Classified Reports Subtotal	4	0	7	3	0	2	2	1	1	4	0	1	0	0	0	1	0	3	1	0	1	0	0
Grand Total	**10**	**3**	**19**	**10**	**5**	**6**	**11**	**7**	**6**	**11**	**0**	**3**	**1**	**2**	**0**	**1**	**2**	**3**	**2**	**1**	**2**	**1**	**0**

Note: Totals do not equal the number of reports identified because one report may cover more than one NIST Cybersecurity Framework Category.

Source: The DoD OIG.

Appendix D

Open Recommendations by NIST Cybersecurity Framework Category

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																						
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
GAO																							
GAO-20-402	1		1															1					
GAO-20-241			3				2							2				1					
GAO-20-129																							
GAO-20-272		1	3						1											1			
GAO-20-299			1																				
GAO-19-457	1		1																				
GAO-20-279																							
GAO-19-570				1																			

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

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																				
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
DoD OIG																							
DODIG-2020-098				1			18		1					5					1				
DODIG-2019-127							1		1										1				
DODIG-2019-116		1								5													
DODIG-2019-105	1		1	1		1	9					4							3				

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

~~(FOUO)~~ Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																		
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Army Audit Agency																							
~~(FOUO)~~ [redacted]	[redacted]																						
~~(FOUO)~~ [redacted]																							
~~(FOUO)~~ [redacted]																							
Naval Audit Service																							
~~(FOUO)~~ [redacted]	[redacted]																						
~~(FOUO)~~ [redacted]																							
~~(FOUO)~~ [redacted]																							

~~(FOUO)~~

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

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																					
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Air Force Audit Agency																							
F2020-0010-O10000																							
F2020-0008-O10000			1						1						1								
F2020-0005-O10000					1																		
F2020-0004-O10000																							
F2020-0003-O10000										2													
F2020-0002-O10000	1		1																				
F2020-0001-O10000	1		2																	1			
F2020-0001-A00900	4		5																				
F2019-0016-A00900			2														1						
F2019-0007-O10000																							
F2019-0014-A00900		1				2																	

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

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																				
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Air Force Audit Agency																							
F2019-0005-L30000			2					1															
F2019-0013-A00900																							
F2019-0012-A00900			1																				
Other DoD Organizations																							
AUD-2019-005-U																							

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

Agency Report No.	NIST Cybersecurity Framework (by Function and Category)																					
	Identify						Protect						Detect			Respond					Recover		
	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	Recovery Planning	Improvements	Communications
Totals																							
Unclassified Reports Subtotal	11	5	30	5	1	4	32	2	4	10	0	4	0	8	1	0	1	2	4	2	0	2	0
Classified Reports Subtotal	16	0	35	25	2	19	25	2	0	29	0	4	0	1	1	0	1	0	12	0	0	0	0
Grand Total	**27**	**5**	**65**	**30**	**3**	**23**	**57**	**4**	**4**	**39**	**0**	**8**	**0**	**9**	**2**	**0**	**2**	**2**	**16**	**2**	**0**	**2**	**0**

Note: Totals do not equal the number of open recommendations identified because one recommendation may cover more than one NIST Cybersecurity Framework Category.
Source: The DoD OIG

Appendix E

Summary of Secret Reports Issued

This appendix contains information about Secret reports issued by the DoD OIG and GAO. Each report identified risks regarding the NIST Cybersecurity Framework. To request access to Appendix E, please file a Freedom of Information Act request online at http://www.dodig.mil/FOIA/Submit-FOIA. To request access to GAO reports, please request online at https://www.gao.gov/reports-testimonies/restricted/request.

Acronyms and Abbreviations

AAA	Army Audit Agency
AFAA	Air Force Audit Agency
AI	Artificial Intelligence
AWCFT	Algorithmic Warfare Cross-Functional Team
CIO	Chief Information Officer
CUI	Controlled Unclassified Information
GAO	Government Accountability Office
IPv6	Internet Protocol Version 6
ISCP	Information System Contingency Plan
JAIC	Joint Artificial Intelligence Center
NFR	Notice of Findings and Recommendations
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
RMF	Risk Management Framework
SAP	Special Access Program


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

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

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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