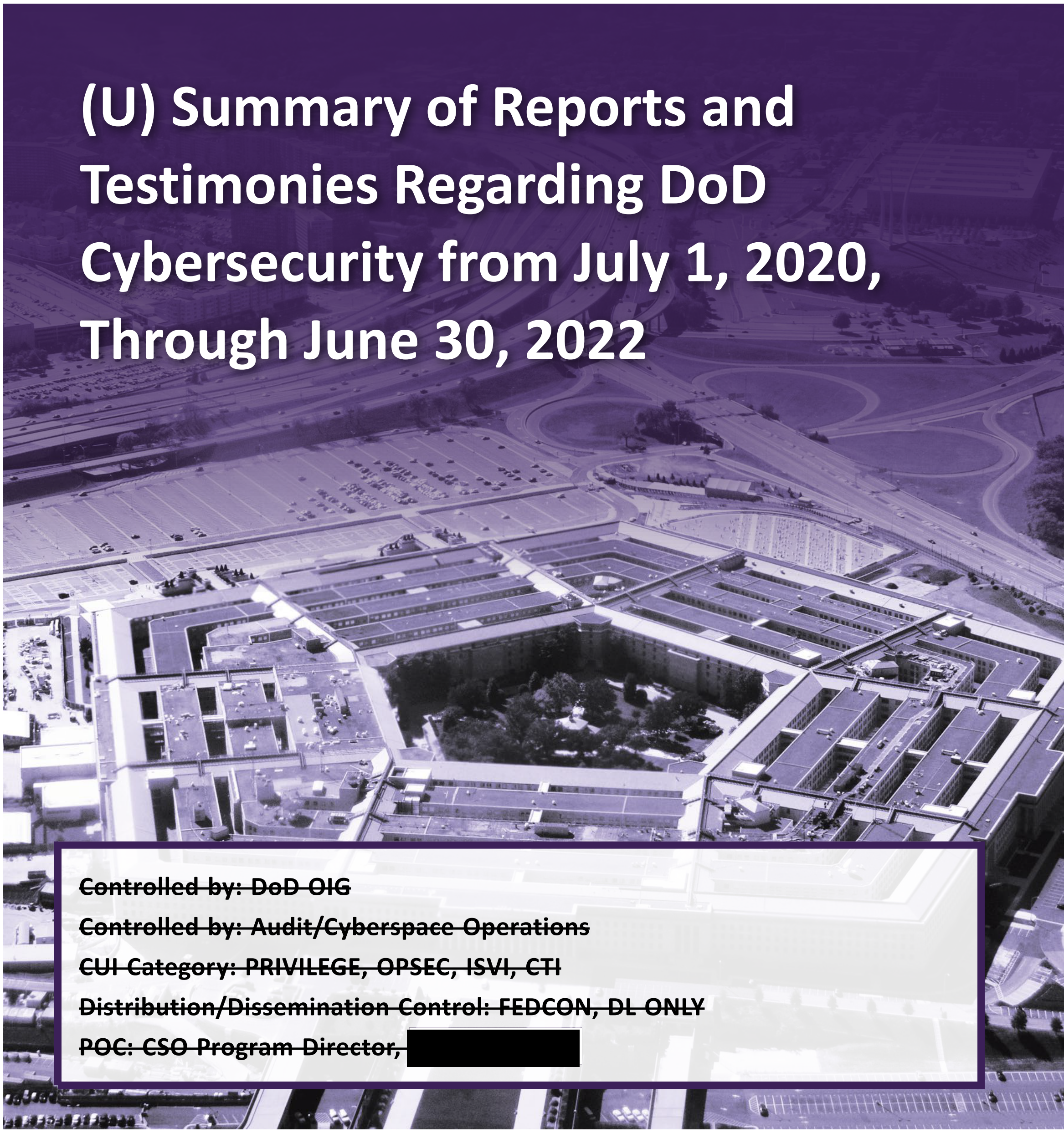
Report No. DODIG-2023-047

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

JANUARY 30, 2023



(U) Summary of Reports and Testimonies Regarding DoD Cybersecurity from July 1, 2020, Through June 30, 2022

~~Controlled by: DoD OIG~~

~~Controlled by: Audit/Cyberspace Operations~~

~~CUI Category: PRIVILEGE, OPSEC, ISVI, CTI~~

~~Distribution/Dissemination Control: FEDCON, DL ONLY~~

~~POC: CSO Program Director,~~ [redacted]

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

~~CUI~~

(U) Results in Brief

(U) Summary of Reports and Testimonies Regarding DoD Cybersecurity from July 1, 2020, Through June 30, 2022

(U) January 30, 2023

(U) Objective

(U) 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 (DoD OIG), the Government Accountability Office (GAO), and other DoD oversight organizations issued between July 1, 2020, and June 30, 2022, concerning DoD cybersecurity; (2) identify cybersecurity trends; and (3) provide a status of open DoD cybersecurity-related recommendations.

(U) We issue this summary report biennially 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.

(U) Background

(U) 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.

(U) Background (cont'd)

(U) Each of the 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."

(U) The DoD also uses the Risk Management Framework, which provides an integrated enterprise-wide decision structure and is consistent with the principles established in the NIST Cybersecurity Framework, for managing cybersecurity risk and authorizing and connecting information systems.

(U) Summary

(U) This year's report summarizes the results of the 133 reports related to DoD cybersecurity—124 unclassified and 9 classified—and 7 congressional testimonies from the DoD OIG, GAO, and other DoD oversight organizations that were released from July 1, 2020, through June 30, 2022.

(U) Over the past 6 years, the DoD OIG, GAO, and the other DoD oversight organizations have steadily increased cybersecurity-related oversight. However, a large and growing percentage of these reports focused primarily on issues related to two of the five NIST Cybersecurity Framework functions—Identify and Protect. There was less oversight provided by the DoD OIG, GAO, and the other DoD oversight organizations of the three remaining NIST Cybersecurity Framework functions—Detect, Respond, and Recover.

(U) The DoD cybersecurity reports issued from July 2020 through June 2022 identified significant challenges in the DoD's management of cybersecurity risks to its systems and networks. The reports discussed DoD risks related to 20 of the 23 NIST Cybersecurity Framework categories. The majority of the weaknesses identified in the 133 reports we reviewed related to the categories of Governance (Identify function), Asset Management (Identify function), Identity Management, Authentication and Access Control (Protect function), and Information Protection Processes and Procedures (Protect function).

(U) Summary (cont'd)

(U) These risks existed because DoD officials did not establish and implement minimum standards and necessary controls in accordance with DoD guidance.

(U) We determined that the DoD Components implemented corrective actions necessary to close 417 of the 895 cybersecurity-related recommendations included in this summary report and prior summary reports. As of June 30, 2022, the DoD had 478 open cybersecurity-related recommendations, dating as far back as 2012.

(U) In addition to the 133 reports and 7 testimonies released since July 1, 2020, we also reviewed the notices of finding and recommendation (NFRs) issued to the DoD as part of the agency financial statement audits and attestations of 26 DoD reporting entities. The NFRs communicate to management identified weaknesses and inefficiencies in financial processes, their impact, the reason they exist, and (U) recommendations on how to correct the weaknesses and inefficiencies. As of July 15, 2022, the DoD had 1,304 open information technology NFRs resulting from FY 2021 financial statement audits. We selected a nonstatistical sample of 44 NFRs and determined that they primarily identified weaknesses in the Protect and Identify functions of the NIST Cybersecurity Framework spanning 11 of the 23 NIST Cybersecurity Framework categories.

(U) 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 such as configuring security settings in accordance with security requirements and developing policies and procedures that promote implementing consistent security controls that address the open cybersecurity-related recommendations.

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

January 30, 2023

(U) MEMORANDUM FOR DISTRIBUTION

(U) SUBJECT: Summary of Reports and Testimonies Regarding DoD Cybersecurity from July 1, 2020, Through June 30, 2022 (Report No. DODIG-2023-047)

(U) 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.

(U) 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.

(U) We appreciate the cooperation and assistance received during the audit. If you have any questions, please contact me at [redacted].

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations & Acquisition,
Contracting, and Sustainment

(U) Distribution:

(U) CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
(U) COMPTROLLER GENERAL, GOVERNMENT ACCOUNTABILITY OFFICE
(U) DIRECTOR, DEFENSE INTELLIGENCE AGENCY
(U) DIRECTOR, NATIONAL GEOSPATIAL-INTELLIGENCE AGENCY
(U) DIRECTOR, NATIONAL SECURITY AGENCY
(U) DIRECTOR, NATIONAL RECONNAISSANCE OFFICE
(U) AUDITOR GENERAL, DEPARTMENT OF THE ARMY
(U) AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE
(U) AUDITOR GENERAL, DEPARTMENT OF THE NAVY

(U) Contents

(U) Introduction

(U) Appendixes

(U) Introduction

(U) Objective

(U) 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 (DoD OIG), the Government Accountability Office (GAO), and other DoD oversight organizations issued between July 1, 2020, and June 30, 2022, concerning DoD cybersecurity; (2) identify cybersecurity trends; and (3) provide a status of open DoD cybersecurity-related recommendations.[1]

(U) 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 (referred to hereafter as the NIST Cybersecurity Framework), for DoD management to review and to consider implementing changes, as appropriate. See Appendix A for a discussion of the scope and methodology and a list of previously issued cybersecurity summary reports. See Appendix B for a list of the reports and testimonies summarized in this report.

(U) Background

(U) The DoD relies on cyberspace, cybersecurity, and cyberspace defense to conduct military, intelligence, and business operations. Cyberspace is a global domain of interdependent networks of information technology (IT) and data, including the Internet, telecommunications networks, and computer systems. Cyberspace security consists of actions taken in cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other IT. Cyberspace defense consists of actions taken in cyberspace to defeat threats that have breached or are threatening to breach cybersecurity measures, including actions to detect and mitigate threats.[2]

[1] (U) Open recommendations can be resolved or unresolved. Resolved recommendations are those DoD management has agreed to implement, but for which management has not yet completed agreed-upon actions. Unresolved recommendations are those DoD management has not agreed to implement or proposed actions that will not address the intent of the recommendation. Closed recommendations are those for which DoD management took corrective action, and the action taken was verified by the oversight organization.

[2] (U) "DoD Dictionary of Military and Associated Terms," November 2022.

(U) According to the 2019 DoD Digital Modernization Strategy, the DoD's enterprise network includes "roughly 10,000 operational systems, thousands of data centers, tens of thousands of servers, millions of computers and IT devices, and hundreds of thousands of commercial mobile devices."[3]

(U) Recent incidents emphasize the need for urgency to improve the Nation's cybersecurity, including the DoD's, as threats rapidly evolve. For example, beginning in September 2019, the Russian Foreign Intelligence Service perpetrated cyber attacks on a software company by injecting hidden code into its network management system, which resulted in that code passing to customers through system updates. Once the systems were updated, malicious actors used a backdoor created by the hidden code to breach impacted information systems.[4] According to the GAO, this attack was not detected until November 2020, when a cybersecurity firm discovered it. In response, the Cybersecurity and Infrastructure Security Agency issued an emergency directive in December 2020. In another example, in May 2021, a foreign criminal hacking group targeted and successfully breached a network that controlled a gas supplier's pipeline. The company proactively shut down systems used to monitor and control the pipeline, causing pipeline operations to halt. At a forum on December 4, 2021, the Commander of the U.S. Cyber Command stated that the cyber attacks on the software company and gas supplier, combined with Russia, China, and Iran's influence and meddling with operations, indicate that the United States "has to compete in cyberspace. We can't stay passive. We have to compete because our adversaries are competing."

(U) In response to these cyber attacks, on May 12, 2021, the President issued Executive Order 14028 requiring the Government to, among other actions, update contracting language on collecting and preserving cybersecurity event data and sharing it Government-wide.[4]

[3] (U) "DoD Digital Modernization Strategy: DoD Information Resource Management Strategic Plan FY19-23," July 12, 2019.

[4] (U) Executive Order 14028, "Improving the Nation's Cybersecurity," May 12, 2021.

(U) DoD Cybersecurity Governance

(U) DoD Instruction 8500.01 establishes the DoD Cybersecurity Program to protect and defend DoD information and IT.[5] Additionally, the Instruction directs the DoD Chief Information Officer to coordinate with NIST to develop cybersecurity-related standards and guidelines. DoD Instruction 8510.01 provides an integrated enterprise-wide risk management structure, known as the DoD Risk Management Framework (RMF).[6] The RMF provides guidance for authorizing and connecting information systems. Specifically, DoD Instruction 8510.01 mandates the use of the RMF for all DoD information technologies and is consistent with the principles established in the NIST Cybersecurity Framework. Cybersecurity risk management comprises the full range of activities undertaken to protect information and IT from cyber threats, such as unauthorized system access and loss of data.

(U) NIST Cybersecurity Framework

(U) 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 United States identify, assess, and manage cyber risk.[7] 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.[8]

(U) To improve accountability for managing enterprise cybersecurity risks further, the President issued Executive Order 13800 in May 2017 requiring Federal agencies to use the NIST Cybersecurity Framework to manage their cybersecurity risk.[9] The Office of Management and Budget also issued guidance in May 2017 to support Federal agencies in implementing Executive Order 13800 requirements.[10]

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

[6] (U) DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022.

[7] (U) Exec. Order No. 13636, 78 Fed. Reg. 11737 (2013).

[8] (U) Public Law 113-274, "Cybersecurity Enhancement Act of 2014," December 18, 2014.

[9] (U) Exec. Order No. 13800, 82 Fed. Reg. 22391 (2017).

[10] (U) Office of Management and Budget M-17-25, "Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 19, 2017.

(U) The NIST Cybersecurity Framework establishes a risk-based approach to managing cybersecurity risk using a common set of cybersecurity activities, desired outcomes, and criteria.[11] Use of the Cybersecurity Framework allows organizations to communicate using a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. The Cybersecurity Framework can also be used to help identify and prioritize actions for reducing cybersecurity risk and to align policy, business, and technological approaches to managing that risk.

(U) Risk Management

(U) The NIST Cybersecurity Framework defines risk management as the ongoing process of identifying, assessing, and responding to risk. Organizations should understand the likelihood that an event, such as unauthorized access that results in stolen or destroyed information, will occur and the potential impacts. Organizations should determine the acceptable level of risk, expressed as their risk tolerance, for achieving their organizational objectives. After establishing the risk tolerance, organizations can then prioritize cybersecurity activities such as updating software and monitoring system access, enabling organizations to make informed decisions about cybersecurity resources.

(U) Organizations can use the NIST Cybersecurity Framework as a key part of their process for identifying, assessing, and managing cybersecurity risk. The NIST Cybersecurity Framework does not replace existing processes; instead, organizations can use their current process and apply the Framework to determine any gaps in their cybersecurity risk approach and develop a roadmap to improvement. Using the Cybersecurity Framework as a cybersecurity risk management tool enables organizations to determine activities that are most important to critical service delivery and prioritize resources to maximize the impact of those activities.

(U) Framework Functions, Categories, and Subcategories

(U) 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

[11] (U) NIST, "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018. For this report, we consider criteria as any informative references as well as industry standards, guidelines, and practices provided by the NIST Cybersecurity Framework.

(U) 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 "plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident." The five NIST Cybersecurity Framework functions comprise 23 associated categories, such as "Asset Management" and 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.

(U) Table 1. NIST Cybersecurity Framework Categories by Function

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

(U) Source: NIST Cybersecurity Framework.

(U) Summary

(U) Cybersecurity Risks Remain a Significant Challenge for the DoD

(U) This year's report summarizes the results of the 133 reports related to DoD cybersecurity—124 unclassified and 9 classified— and 7 congressional testimonies by the DoD OIG, GAO, and other DoD oversight organizations that were released from July 1, 2020, through June 30, 2022.[12]

(U) Over the past 6 years, the DoD OIG, GAO, and the other DoD oversight organizations have steadily increased cybersecurity-related oversight, demonstrated by the increasing number of cybersecurity-related reports issued and testimonies made during this period. For example, in the 2-year period from July 2020 through June 2022, oversight organizations issued 133 DoD cybersecurity-related reports compared to the 90 reports issued in the 2-year period from July 2018 through June 2020 and 53 reports issued in the 2-year period from July 2016 through June 2018. However, a large and growing percentage of these reports focused on issues related to two of the five NIST Cybersecurity Framework functions—Identify and Protect. There was less oversight provided by the DoD OIG, GAO, and the other DoD oversight organizations of the three remaining NIST Cybersecurity Framework functions—Detect, Respond, and Recover.

(U) We determined that despite improvements made by the DoD, cybersecurity reports issued during the past 2 years demonstrate that the DoD continues to face significant challenges in managing cybersecurity risks to its systems and networks. For example, we determined the reports pertained to DoD risks regarding 20 of the 23 NIST Cybersecurity Framework categories. The majority of the weaknesses identified in the 133 reports we reviewed related to three categories: Governance (Identify function); Asset Management (Identify function); and Identity Management, Authentication and Access Control (Protect function). See Appendix C for a list of reports and testimonies identifying cybersecurity risks by the NIST Cybersecurity Framework category.

(U) The risks existed because DoD officials did not establish policies and procedures to implement minimum standards, or did not effectively implement the necessary controls, in accordance with DoD and Federal guidance.

[12] (U) See Appendix B for a list of all reports and testimonies regarding DoD cybersecurity issues during this period.

(U) We also determined that DoD Components implemented corrective actions necessary to close 417 of the 895 cybersecurity-related recommendations included in this summary report and prior summary reports.[13] Those corrective actions mitigated or remedied cybersecurity risks and weaknesses to DoD systems and networks. However, as of June 30, 2022, the DoD had 478 open cybersecurity-related recommendations, dating as far back as 2012.[14]

(U) In addition to the 133 reports and 7 testimonies released from July 1, 2020, through July 15, 2022, the DoD had 1,304 open IT Notices of Findings and Recommendations (NFRs) resulting from the FY 2021 DoD financial statement audits.[15] From a nonstatistical sample of 44 IT NFRs, we determined that 21 of the IT NFRs directly related to the NIST Cybersecurity Framework category of Identity Management Authentication and Access Control (Protect function), and 16 of the IT NFRs directly related to Governance category (Identify function).

(U) Lack of effective system controls can result in significant risk to DoD assets. For example, payments and collections could be lost, stolen, or duplicated because of weak IT controls. Implementing the recommended actions included in the IT 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 IT systems that process financial transactions can improve financial management and the overall cybersecurity of the DoD Information Network.[16]

(U) 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 implements timely and comprehensive corrective actions to address open cybersecurity-related recommendations. Adversaries such as Russia, China, Iran, and North Korea; terrorist groups; hacktivists; and other independent malicious actors have exploited 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,

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

[14] (U) See Appendix D for a matrix of open recommendations identifying cybersecurity risks consistent with each NIST Cybersecurity Framework function and category.

[15] (U) IT NFRs communicate to management in a timely manner any identified internal control weaknesses and inefficiencies in IT systems impacting 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.

[16] (U) The DoD Information Network is the globally interconnected set of information capabilities and communications and computing systems and services.

(U) and conduct cyber-attacks.[17] Additionally, the DoD OIG continues to identify cybersecurity related risks as a major challenge facing the DoD, and has included it in the Top DoD Management Challenges for the past five years.[18]

(U) Increased DoD Cybersecurity Oversight

(U) The DoD OIG, GAO, and other DoD oversight organizations have steadily increased cybersecurity-related oversight by issuing more cybersecurity-related reports over the past 6 years. However, a large and growing percentage of these reports focused on only two of the five NIST Cybersecurity Framework functions—Identify and Protect.

(U) As shown in Table 2, organizations overseeing the DoD issued an increasing number of cybersecurity-related reports each year from July 2016 through June 2022, despite some 1-year decreases.

(U) Table 2. Number of DoD Cybersecurity-Related Reports Issued by Oversight Organizations Since July 1, 2016

(U) Period	GAO	DoD OIG	Army Audit Agency	Naval Audit Service	Air Force Audit Agency	Other DoD Agencies	Total
July 1, 2016, through June 30, 2017	9	6	3	0	9	2	29
July 1, 2017, through June 30, 2018	7	6	0	2	7	2	24
July 1, 2018, through June 30, 2019	11	12	4	5	6	8	46
July 1, 2019, through June 30, 2020	9	9	3	3	14	6	44
July 1, 2020, through June 30, 2021	14	8	8	6	19	4	59
July 1, 2021, through June 30, 2022	9	9	8	5	35	8	74
Total	**59**	**50**	**26**	**22**	**90**	**30**	**276** **(U)**

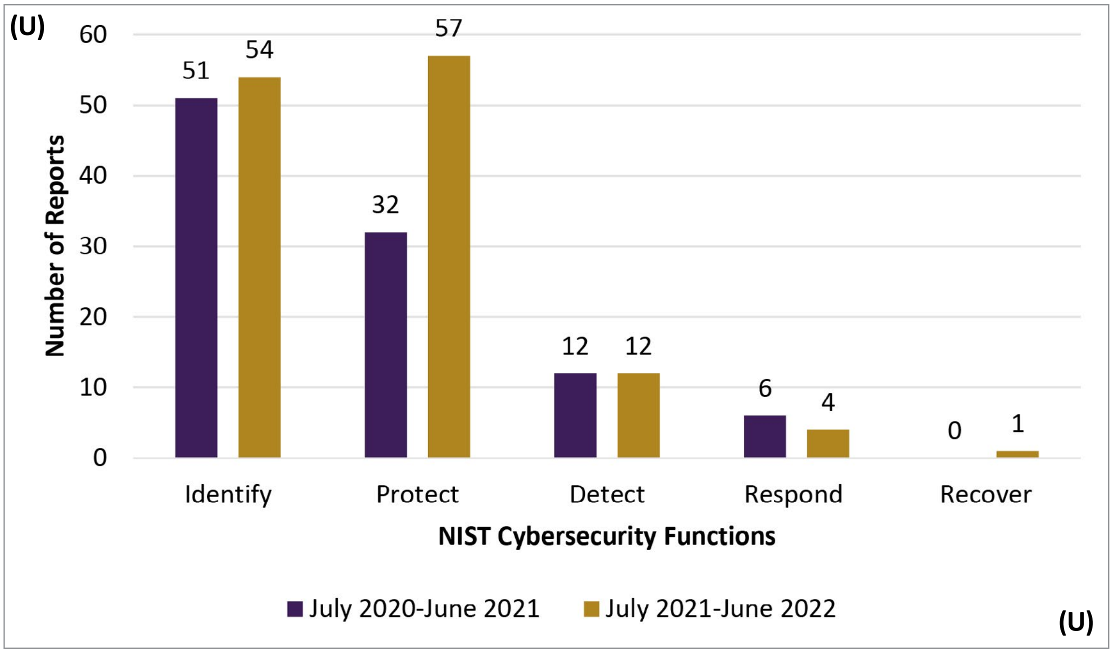
(U) Source: The DoD OIG.

[17] (U) The Cybersecurity and Infrastructure Security Agency defines hacktivists as politically active hackers, whose goal is to cause damage to achieve notoriety for their cause.

[18] (U) DoD OIG, "Fiscal Year 2022 Top DoD Management Challenges," October 15, 2021; DoD OIG, "Fiscal Year 2021 Top DoD Management Challenges," October 15, 2020; andDoD OIG, "Fiscal Year 2020 Top DoD Management Challenges," October 15, 2019;DoD OIG, "Fiscal Year 2019 Top DoD Management Challenges," October 15, 2018; andDoD OIG, "Fiscal Year 2018 Top DoD Management Challenges," November 20, 2017.

(U) From July 2016 through June 2022, most cybersecurity-related reports issued by DoD oversight organizations were related to the Identify and Protect functions. Specifically, 225 cybersecurity-related reports were related to the Identify function, 184 were related to the Protect function, while only 75 were related to the Detect, Respond, and Recover functions combined. Figure 1 shows cybersecurity-related reports by NIST Cybersecurity Framework function since July 2020.

(U) Figure 1. Reports from July 2020 through June 2022 by NIST Cybersecurity Framework Function



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

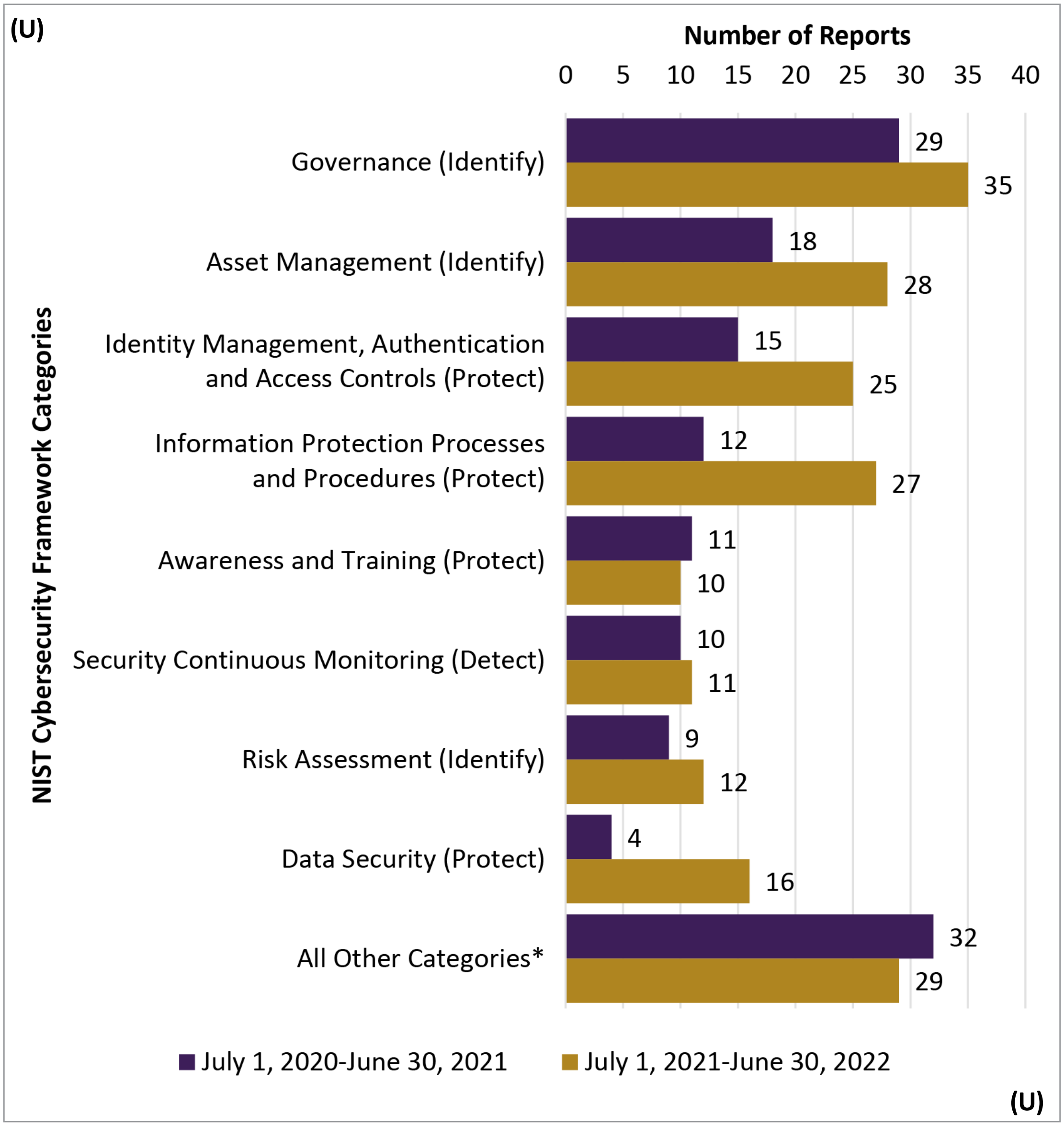
(U) Source: The DoD OIG.

(U) Specifically, from July 2020 through June 2022, of the 133 cybersecurity related reports:

- (U) 105 were related to the Identify function – manage cybersecurity risks to systems, people, assets, data, and capabilities, and the ability to prioritize efforts to manage cybersecurity risks;
- (U) 89 were related to the Protect function – develop and implement cybersecurity safeguards that support the ability to limit or contain the impact of potential cybersecurity events;
- (U) 24 were related to the Detect function – activities that identify a cybersecurity event in a timely manner;
- (U) 10 were related to the Respond function – contain the impact of a cybersecurity incident; and
- (U) 1 was related to the Recover function – maintain resilience and enable timely recovery from a cybersecurity incident.

(U) From July 2020 through June 2022, most cybersecurity-related reports issued by DoD oversight organizations were related to three categories: Governance (Identify function); Asset Management (Identify function); and Identity Management, Authentication, and Access Control (Protect function). Figure 2 shows the number of reports that identify risks and findings by NIST Cybersecurity Framework category.

(U) Figure 2. Number of Unclassified and Classified Reports with Risks Identified by NIST Cybersecurity Framework Category (from July 1, 2020, through June 30, 2022)



* (U) The "All Other Categories" column comprises 15 of the 23 NIST Cybersecurity Framework categories.

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

(U) Source: The DoD OIG.

(U) We summarized the three categories, identified the number of reports and open recommendations associated with each category, and presented examples.

(U) Governance Category

(U) The NIST Cybersecurity Framework defines Governance as policies and procedures necessary to manage and monitor an organization's operational requirements and cybersecurity risks. Governance category findings and recommendations identified in 64 reports in this year's summary included DoD Components issuing conflicting cybersecurity guidance for managing risk and not consistently implementing requirements for using vulnerability identification tools such as antivirus scanning software. By implementing the 92 open recommendations relevant to this category, the DoD can improve its management of cybersecurity risk through implementing all relevant policies, procedures, and processes used to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements.

(U) Asset Management Category

(U) The NIST Cybersecurity Framework defines Asset Management as the identification and management of data, personnel, systems, devices, and facilities consistent with their importance to an organization's risk strategy. Asset Management category findings and recommendations identified in the 46 reports in this year's summary included DoD Components not having controls to collect and share data identifying personnel and information security responsibilities, and maintaining system and device inventories. By implementing the 35 open recommendations relevant to this category, the DoD could improve its ability to manage and identify assets to achieve organizational objectives.

(U) Identity Management, Authentication, and Access Control Category

(U) The NIST Cybersecurity Framework defines Identity Management, Authentication, and Access Control as the ability to manage physical and logical access to assets and facilities consistent with assessed risk. Identity Management, Authentication, and Access control category findings and recommendations identified in the 40 reports in this year's summary included DoD Components allowing user access to systems without a documented need for access. By implementing the 42 open recommendations relevant to this category, the DoD can improve its ability to prevent unauthorized access to DoD systems and networks.

(U) Ultimately, the DoD must ensure that it identifies and manages its cybersecurity-related risks appropriately to protect people, assets, data, and capabilities from constantly evolving and increasingly sophisticated cybersecurity threats.

(U) The DoD Took Actions to Improve DoD Cybersecurity

(U) DoD Components took corrective actions during the past 2 years sufficient for oversight entities to close 417 cybersecurity-related recommendations that addressed a variety of cybersecurity risks, as illustrated in the following examples:

- (~~CUI~~) [redacted]
- (U) In a 2021 report, the DoD OIG recommended that DoD officials include additive manufacturing systems in the IT systems portfolio and establish and maintain cybersecurity controls in accordance with Federal and DoD guidance.[20] To address the recommendation, the DoD CIO, Under Secretary of Defense for Research and Engineering, and the Under Secretary of Defense for Acquisition and Sustainment updated the IT systems portfolio and established cybersecurity controls in accordance with Federal and DoD guidance. These actions resulted in additive manufacturing system owners having to establish security controls and obtain an authority to operate to minimize cybersecurity risk.
- (U) In a 2021 report, the GAO recommended that the DoD establish a process for formally communicating future critical acquisition programs and technologies lists to all relevant DoD organizations and Federal agencies.[21] The DoD disseminated an Critical Programs and Technologies list to internal and external stakeholders. This action resulted in a more

[19] (~~CUI~~) [redacted]

[20] (U) DoD OIG Report DoDIG-2021-098, "Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems," July 1, 2021.

[21] (U) GAO Report No. GAO-21-158, "DoD Critical Technologies: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed," January 12, 2021.

(U) consistent and enterprise-wide understanding of DoD critical technologies and the necessity to implement security controls to protect them from cybersecurity risks.

- (U) In a 2021 report, the Army Audit Agency (AAA) recommended that the Deputy Assistant Secretary of the Army-Budget establish structured processes across all Army appropriations that require commands to identify unfunded IT requirements.[22] To address the recommendation, the Army Budget Office established an automated unfunded requirement portal in January 2021 that requires users to select a block in the portal that specifically identifies IT requirements. This action improved the Army's ability to more consistently identify and track its current and future IT funding needs.
- (~~CUI~~) [redacted]

(U) DoD Components have taken corrective actions to comply with requirements and standards. However, cybersecurity reports identify that the DoD continues to face significant challenges in managing and improving its overall cybersecurity posture. As of June 30, 2022, the DoD had 478 open cybersecurity-related recommendations—317 unclassified and 161 classified—that have been open as far back as 2012.

(U) Cyber attacks are becoming more sophisticated, malicious tools are becoming more prevalent, and IT systems, networks, and devices are becoming more interconnected. The DoD must ensure that it takes corrective actions on all open recommendations. The longer it takes the DoD to implement corrective actions, the more likely it is that DoD cybersecurity vulnerabilities and threats could be exploited, causing security incidents that disrupt critical operations; leading to inappropriate access to and disclosure, modification, or destruction of sensitive and classified information; and threatening national security.

[22] (U) AAA Report No. A-2021-0051-AXZ, "Information Technology Spend – Unfunded Requirements," June 1, 2021.

[23] (~~CUI~~) [redacted]

(U) Challenges Remain in Managing DoD Cybersecurity Risks

(U) This year's summary report highlights, as did previous summary reports, that the DoD needs to continue focusing corrective actions on cybersecurity weaknesses affecting the NIST Cybersecurity Framework Identify and Protect Functions.

(~~CUI~~) Based on the reports included in this year's summary report, we determined that the Identify function, in particular the Governance category, had the most reported cybersecurity risks or weaknesses. Specifically, 64 of the 133 issued reports identified that DoD officials did not have effective controls in place or take the needed steps to ensure that DoD Components fully implemented established policies and procedures. [redacted].[24] Without cybersecurity governance, DoD Components limit their ability to consistently and effectively implement cybersecurity requirements necessary to protect DoD networks and operations from being compromised.

(U) Additionally, 40 reports identified cybersecurity risks with limiting access to authorized officials (Identity Management, Authentication and Access Control category), 39 reports identified risks with developing and maintaining security policies, processes, and procedures (Information Protection Processes and Procedures category), and 46 reports identified risks with identifying and managing assets (Asset Management category). Without effectively implemented security controls in those areas, the DoD cannot ensure that:

- (U) only authorized users access information on the DoD Information Network;
- (U) devices are properly configured in accordance with DoD and Federal requirements; and
- (U) personnel can implement security controls effectively and mitigate risks accordingly.

[24] (U) AFAA Report No. F2022-0002-O10000, "Protection of Technical and Proprietary Data," December 1, 2021.

(U) Risks by NIST Cybersecurity Framework Function

(U) The 133 reports identified cybersecurity risks in all five NIST Cybersecurity Framework functions – Identify, Protect, Detect, Respond, and Recover. The seven congressional testimonies discussed cybersecurity risks in the Identify, Protect, Detect, and Respond functions. Table 3 summarizes the number of unclassified and classified reports, by oversight agency, that included findings related to specific NIST Cybersecurity Framework functions.[25]

(U) Table 3. Number of Unclassified and Classified Reports by NIST Cybersecurity Framework Function

(U) Function	GAO	DoD OIG	Army Audit Agency	Naval Audit Service	Air Force Audit Agency	Other DoD Agencies	Total
Identify	21	14	14	7	37	12	**105**
Protect	11	8	7	5	47	11	**89**
Detect	2	3	1	0	14	3	**24**
Respond	2	0	1	2	3	2	**10**
Recover	0	0	0	0	1	0	**1** **(U)**

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

(U) Source: The DoD OIG.

(U) Identify Function

(U) We determined there were 105 unclassified and classified reports, and seven testimonies that identified cybersecurity risks regarding the Identify function. The Identify function includes activities that develop an organizational understanding for managing cybersecurity risk to systems, people, assets, data, and capabilities. These activities enable organizations to focus and prioritize efforts according to their risk management strategies and business needs. The reports and testimonies identified risks and weaknesses regarding the Identify function that limited the DoD's ability to manage cybersecurity risks effectively, such as not establishing and communicating cybersecurity policy throughout DoD organizations. Table 4 provides the NIST Cybersecurity Framework categories under the Identify function, the desired cybersecurity outcomes, and the number of reports and testimonies per category.

[25] (U) We account for the issues related to each NIST Cybersecurity Framework function that we identified in the classified reports we reviewed in Table 3. We did not summarize the issues in separate classified appendices because none of the issues included in those reports were different from what we reported in this summary.

(U) Table 4. NIST Cybersecurity Framework Categories for the Identify Function

(U) Category	Cybersecurity Outcomes	Number of Reports	Number of Testimonies
Asset Management	Organizations identify and manage data, personnel, devices, systems, and facilities to achieve business purposes consistent with their relative importance to objectives and risk strategy.	46	1
Business Environment	Organizations understand and prioritize the mission, objectives, stakeholders, and activities to inform cybersecurity roles, responsibilities, and risk management decisions.	5	3
Governance	Organizations understand policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements.	64	2
Risk Assessment	Organizations understand cybersecurity risk to operations (including mission, functions, image, or reputation), assets, and individuals.	21	1
Risk Management Strategy	Organizations establish and implement priorities, constraints, risk tolerances, and assumptions to support operational risk decisions.	17	0
Supply Chain Risk Management	Organizations establish and implement priorities, constraints, risk tolerances, and assumptions to identify, assess, and manage supply chain risk.	7	0 **(U)**

(U) Note: Totals may not equal the number of reports or testimonies identified because one may cover more than one NIST Cybersecurity Framework function.

(U) Source: NIST Cybersecurity Framework.

(U) The following sections provide examples of cybersecurity risks from unclassified reports pertaining to the Identify function. For each category, we summarize examples of related reports' findings, causes, effects, and recommendations.

(U) Asset Management Category

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

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

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) DoD OIG Report No. DODIG-2021-110, "Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce," July 29, 2021

(U) The DoD OIG determined that the Office of the DoD CIO took action to meet strategic goals for the recruitment and retention of its civilian cyber workforce. However, DoD Components did not code or incorrectly coded some of their civilian cyber workforce positions. The work role coding was incomplete or incorrect for four of the five DoD Components reviewed because they did not have a quality assurance process to ensure that role coding complied with the DoD Coding Guide.

(U) The DoD OIG concluded that the DoD may be unable to accurately determine the skill set and size of its civilian cyber workforce. Without complete and correct coding of all civilian cyber workforce positions, the DoD may develop incorrect workforce planning activities, such as recruitment and retention strategies, and incorrectly report on work roles that the DoD critically needs.

(U) The DoD OIG made three recommendations concerning DoD coding guidance for cyber workforce positions, including that the DoD CIO require DoD Components to code filled and unfilled cyber workforce positions to meet Federal requirements. As of August 2022, all recommendations were resolved and remained open.

(U) Business Environment Category

(U) Government Accountability Office Report No. GAO-20-249SP, "Information Technology: Key Attributes of Essential Federal Mission-Critical Acquisitions," September 8, 2020

(U) The GAO determined that the DoD identified risk factors and challenges related to the DoD's Defense Healthcare Management System Modernization program, including shared governance, obtaining adequate resources, and workforce issues.

(U) For example, the GAO reported that DoD and Department of Veteran Affairs programs and operations shared governance as a potential program risk. The GAO also reported that DoD officials stated that the lack of a joint, enterprise-level, multi-faceted, structured, functional, and technical Department of Veterans Affairs and DoD governance plan put the DoD at risk of execution failures, as well as cost, schedule, and performance delays. The GAO further reported that the DoD identified that, if it did not obtain Government and contractor resources necessary to support the current deployment model, it would not be able to provide adequate oversight of the Defense Healthcare Management System Modernization during deployments.

(U) The GAO did not make recommendations to the DoD in this report.

(U) Government Accountability Office Report No. GAO-21-182, "DoD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule," December 23, 2020

(U) The GAO determined that 10 of 15 selected programs had delays in their planned schedules. Schedule delays ranged from 1 month to 5 years. The GAO reported that program officials cited cybersecurity and system performance issues and maintenance and budget approval processes as reasons for delays.

(U) The GAO also reported programs did not consistently implement specific practices, contributing to program risks that might affect cost and schedule outcomes. Specifically, the GAO reported that although all 15 programs had cybersecurity strategies, officials from only 8 programs conducted systematic

(U) examinations of information systems to identify security deficiencies. When systematic examination was conducted, fewer cost increases and schedule delays occurred.

(U) The GAO did not make recommendations to the DoD in this report.

(U) Governance Category

(U) Army Audit Agency Report No. A-2021-0038-AXZ, "Information Technology Spend – Investment Threshold and Equipment Accountability Policy," April 5, 2021

(U) The AAA determined that the Army had limited visibility of Operations and Maintenance, Army IT purchases exceeding $250,000. Specifically, the AAA identified 952 purchases, totaling about $2.7 billion, for IT equipment and services during FYs 2018 and 2019 across 34 organizations exceeding the $250,000 threshold. The AAA reviewed 67 sampled purchases totaling $79 million and identified vague expenditure descriptions and a lack of supporting documentation in the Army's General Fund Enterprise Business System, which prevented the AAA from verifying whether the purchases violated the threshold policy. In addition, the AAA identified inconsistencies in how organizations made investment determinations and interpreted qualifications for using Operations and Maintenance, Army and Other Procurement, Army dollars. The AAA also determined that the Army's property accountability policies did not support IT equipment visibility, and the Army did not consistently manage equipment in a property system of record.

(U) The AAA reported that the Army did not have data standards to facilitate timely, comprehensive, and accurate use of the Army's General Fund Enterprise Business System data by all users. The AAA reported that organizations used vague terminology to describe expenditures in the General Fund Enterprise Business System and did not make supporting documentation readily available.

(U) The AAA concluded using unclear and inaccurate terminology compromised the integrity and reliability of Army financial data and systems. Additionally, the AAA concluded that the Army could not inventory IT equipment as it did for other non-IT assets and that the irregularities in criteria could create duplicative purchases and excess inventory.

(U) The AAA made six recommendations concerning IT procurements and visibility of IT assets, including that the Army CIO develop guidance on conducting legal reviews of IT procurements exceeding $250,000. As of August 2022, two recommendations were closed, and the remaining four were resolved and remained open.

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Risk Assessment Category

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

~~(CUI)~~ [redacted]

(U) Army Audit Agency Report No. A-2022-0033-IIZ, "Cloud Migration," March 14, 2022

(U) The AAA determined that Army organizations did not consistently rationalize and complete IT investment analyses for their systems, applications, and data before migrating them to a cloud environment.[26] The AAA reviewed 50 of the 222 systems reported in the Army Portfolio Management Solution that were identified as being hosted in a cloud environment and determined that Army organizations did not rationalize 22 (44 percent) and did not complete IT investment analyses for 19 (38 percent) systems reviewed. In addition, the AAA determined that the Army decommissioned three systems after migrating them to a cloud environment without rationalizing or completing IT investment analyses before decommissioning.

(U) The AAA reported that Army guidance lacked detailed processes and procedures for organizations to complete rationalization and investment analyses; leaders provided contradicting or unclear direction on which systems required rationalization and IT investment analyses; and organizations lacked cloud-specific knowledge and skills to rationalize systems and complete investment analyses.

(U) The AAA concluded that Army organizations did not consolidate or decommission systems and projected that the Army programmed $1.15 billion for systems that it did not rationalize and $812.9 million for systems without

[26] (U) In Report A-2022-0033-IIZ, the AAA defined rationalization as the systematic management of IT investments to identify value-added applications and eliminate outdated, legacy, and duplicative applications.

(U) IT investment analyses. The AAA concluded these issues reduced the Army's ability to achieve its cloud rationalization and migration efforts or meet DoD and Army cloud and modernization goals.

(U) The AAA made six recommendations concerning rationalization guidance and IT investment analyses, including for the Army CIO to issue guidance requiring organizations to reassess their systems after migration to ensure the systems were needed. As of August 2022, one recommendation was closed, and the remaining five were resolved and remained open.

(U) Risk Management Strategy Category

(U) DoD Office of Inspector General Report No. DODIG-2022-041, "Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process," December 3, 2021

(U) The DoD OIG determined that the U.S. Transportation Command and the Defense Health Agency leveraged reciprocity while authorizing their systems through the RMF process by making their systems and authorization documentation available in enterprise Mission Assurance Support Service. The DoD OIG also determined that those agencies appointed enterprise Mission Assurance Support Service reciprocity users, and authorized Tier 2 common controls in accordance with Federal and DoD guidance; however, the Defense Logistics Agency and Defense Human Resources Activity did not.

(U) The DoD OIG reported that the Defense Logistics Agency believed its systems had unique missions and were relevant only to agency personnel, and did not consider the DoD's RMF and reciprocity policy and implementation guidance to be a priority. The DoD OIG also reported that the Defense Human Resources Agency was reorganizing and its director had not yet assigned and documented cybersecurity roles and responsibilities for implementing RMF and reciprocity requirements.

(U) The DoD OIG concluded that unless DoD Components fully leverage RMF reciprocity, they may not fully realize the associated benefits, including faster deployment of secure systems and cost savings.

(U) The DoD OIG made three recommendations concerning improvements to leverage reciprocity, including for the DoD CIO to revise existing guidance or issue new guidance requiring system program managers to certify that they consider reciprocity before authorizing and reauthorizing systems. As of August 2022, all recommendations were resolved and remained open.

(U) Air Force Audit Agency Report No. F2021-0007-REA000, "Software Use 20th Fighter Wing Shaw AFB, SC," January 11, 2021

(U) The AFAA determined that 20th Fighter Wing officials did not maintain licensed, approved, and current software on Air Force networks. After reviewing 50 non-enterprise and 80 sampled software assets, the AFAA determined the software license manager did not maintain documentation identifying the number of authorized users and software expiration dates for all non-enterprise and four sampled software assets. In addition, the AAFA determined that officials obtained approval for software placement on Air Force networks, but did not track expiration dates for all non-enterprise and four sampled software assets. Furthermore, the AFAA determined that the previous base software manager did not inventory software assets on Air Force networks, and cybersecurity officials did not complete vulnerability assessments and remediate repeat vulnerabilities on the assets.

(U) The AFAA reported that 20th Communications Squadron leadership did not verify that the software license manager performed annual inventories for all software licenses and maintain license documentation and proof of purchase and Government rights as required.

(U) The AFAA concluded that the 20th Fighter Wing did not accurately maintain licensed, approved, and current software on the Air Force network infrastructure. Maintaining licensed, approved, and current software is essential to mitigating cyber attacks and unauthorized network access from insider and outsider threats.

(U) The AFAA made three recommendations to improve software management, including for the software license manager to ensure organizations conducted and documented annual inventories for all non-enterprise and unidentified software licenses and maintained software licenses and proof of software purchases and Government rights. These recommendations are closed.

(U) Supply Chain Risk Management Category

(U) DoD Office of Inspector General Report No. DODIG-2021-125, "Evaluation of U.S. Special Operations Command's Supply Chain Risk Management for the Security, Acquisition, and Delivery of Specialized Equipment," September 14, 2021

(U) The DoD OIG determined that the U.S. Special Operations Command issued a revised supply chain risk management policy in November 2020 that meets DoD requirements, which includes making Program Protection Plans

(U) and Program Protection Implementation Plans mandatory for the command's acquisitions. However, U.S. Special Operations Forces, Acquisition, Technology, and Logistics officials did not have a plan to develop Program Protection Plans and Protection Implementation Plans for contracts awarded before the issuance of the November 2020 policy and did not provide Program Protection Plans for 26 of the 43, or 60 percent, of specialized equipment acquisitions reviewed.

(U) The DoD OIG concluded that not having Program Protection Plans for all acquisitions introduced significant risk to the U.S. Special Operations Command's ability to identify, assess, and mitigate supply chain risk.

(U) The DoD OIG made five recommendations concerning improvements to manage supply chain risk, including for the U.S. Special Operations Command Special Operations Forces Acquisition, Technology, and Logistics Center to identify which acquisitions did not have Program Protection Plans in place as required by DoD guidance. As of August 2022, two recommendations were closed, and the remaining three were resolved and remained open.

(U) Army Audit Agency Report No. A-2022-0015-AXZ, "Portable Electronic Devices and Wireless Services Management," December 10, 2021

(U) The AAA determined that two commands—the U.S. Army Reserve Command and the U.S. Army Corps of Engineers—generally followed guidance and policies when acquiring and managing 30,000 portable electronic devices and associated wireless services to support mission requirements. Although the AAA determined that both commands acquired the portable electronic devices from approved sources, neither command could provide documentation to support their visibility of 40 percent and 70 percent, respectively, of sampled portable electronic devices acquired during FY 2019 and FY 2020.

(U) The AAA reported that U.S. Army Reserve Command officials did not record portable electronic devices in the property system of record using a unique identifier and U.S. Army Corps of Engineers officials were not required to record portable electronic devices in the property system of record using a unique identifier before FY 2020. In addition, the AAA reported that since FY 2020, the U.S. Army Corps of Engineers used serial numbers to track portable electronic devices instead of international mobile equipment identity numbers, which vendors use for tracking devices and developing vendor usage reports.

(U) The AAA concluded that having limited visibility of portable electronic devices meant neither command had control of the devices paid for each month and increased the risk of these devices being lost or stolen.

(U) The AAA made three recommendations concerning the management of wireless services, including for the Deputy Chief of Staff for Logistics (G-4) to revise Army guidance to account for all portable electronic devices in the Army's property system of record using a unique device identifier. As of August 2022, one recommendation was closed, and the remaining two were resolved and remained open.

(U) Protect Function

(U) We determined there were 89 unclassified and classified reports and 2 testimonies that identified cybersecurity risks regarding the Protect function. The Protect function includes activities that help organizations develop and implement appropriate safeguards to deliver critical services. The reports and testimonies identified risks and weaknesses, such as inconsistent implementation of security controls to safeguard information that limited the DoD's ability to manage cybersecurity risks effectively. Table 5 provides the NIST Cybersecurity Framework categories under the Protect function, the corresponding cybersecurity outcomes, and the number of reports and testimonies per category.

(U) Table 5. NIST Cybersecurity Framework Categories for the Protect Function

(U) Category	Cybersecurity Outcomes	Number of Reports	Number of Testimonies
Identity Management, Authentication, and Access Control	Organizations limit access to physical and logical assets and facilities to authorized users, processes, and devices, consistent with the assessed risk of unauthorized access to authorized activities and transactions.	40	1
Awareness and Training	Organizations provide personnel and partners cybersecurity awareness education and training to perform their cybersecurity-related duties and responsibilities consistent with policies, procedures, and agreements.	21	0
Data Security	Organizations manage information and records (data) consistent with risk strategy to protect the confidentiality, integrity, and availability of information.	20	1 (U)

(U) Table 5. NIST Cybersecurity Framework Categories for the Protect Function (cont'd)

(U) Category	Cybersecurity Outcomes	Number of Reports	Number of Testimonies
Information Protection Processes and Procedures	Organizations maintain and implement security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures to protect information systems and assets.	39	1
Maintenance	Organizations perform maintenance and repairs of industrial control and information system components consistent with policies and procedures.	2	0
Protective Technology	Organizations manage technical security solutions to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	13	0 (U)

(U) Note: Totals may not equal the number of reports or testimonies identified because one may cover more than one NIST Cybersecurity Framework function.

(U) Source: NIST Cybersecurity Framework.

(U) The following sections provide examples of cybersecurity risks from unclassified reports and a testimony pertaining to the Protect function. For each category, we summarize examples of related reports' findings, causes, effects, and recommendations.

(U) Identity Management, Authentication, and Access Control Category

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) "Future Cybersecurity Architectures," Joint DoD Statement Before the Senate Armed Services Committee - Subcommittee on Cybersecurity, April 14, 2021

(U) In a joint statement before the Senate Armed Services Committee, Subcommittee on Cybersecurity, the DoD Deputy CIO for Cybersecurity and Chief Information Security Officer, the National Security Agency Cybersecurity Directorate Director, and the DoD Deputy Principal Cyber Advisor testified about the DoD's response to server incidents involving two software companies, and its plans to implement a Zero Trust Framework across the DoD Information Network.

(U) DoD officials testified that these server incidents demonstrated the increasing sophistication, determination, and resourcefulness of cyberspace adversaries and the DoD's need to assume the DoD Information Network has been compromised. DoD officials testified that the DoD's Zero Trust Framework is being built on a "deny by default" security model.

(U) DoD officials also testified that implementing a Zero Trust Framework would mitigate the issues brought to light in the server incidents by only allowing access to data if the user and device are authorized and authenticated.

(U) Awareness and Training Category

(U) Air Force Audit Agency Report No. F2021-0008-REG000, "Integrated Base Defense Security System – Risk Management Framework 96th Test Wing Eglin AFB, FL," December 1, 2020

(U) The AFAA determined that 96th Security Forces Squadron, Installation Security Office officials did not comply with RMF continuous security control monitoring requirements for the Integrated Base Defense Security Systems at Eglin Air Force Base. Specifically, the AFAA identified that officials did not maintain required records for a specific system that documented the purchase and installation of system hardware components and alarms in their authorization boundaries. Additionally, the AFAA identified that officials could not provide system architecture records that documented accurate as-built drawings for the system. The AFAA also identified that the 96th Security Forces Squadron did not keep records on site and instead allowed the contractor to store the system architecture records at its facility.

(U) The AFAA reported that 96th Security Forces Squadron, Installation Security Office officials did not receive adequate technical training to evaluate contractor support related to the RMF, such as conducting preventative maintenance tasks and testing system access controls.

(U) The AFAA concluded that complying with RMF requirements ensures critical base defense systems protect Air Force installations from exposure to physical and cyber threats. The AFAA also concluded that compliance enhances operational reliability critical for executing the Security Forces mission.

(U) The AFAA made five recommendations concerning improvements to security controls continuous monitoring, including for the 96th Security Forces Squadron Commander to establish procedures to maintain records for documenting purchases and the installation of system hardware components. These recommendations are closed.

(U) Air Force Audit Agency Report No. F2021-0002-RES000, "Integrated Base Defense Security System Risk Management Framework 78th Air Base Wing, Robins AFB, GA," November 4, 2020

(U) The AFAA determined that 78th Security Forces Squadron officials coordinated with the Air Force Life Cycle Management Center, Force Protection Division, to complete the RMF accreditation requirements at Robins Air Force Base. However, they did not obtain reauthorization or an acceptance

(U) memorandum for the Integrated Base Defense Security System's authority to operate, nor did they verify personnel performed periodic cybersecurity reviews, testing, and annual assessments of system compliance.

(U) The AFAA reported that Air Force guidance did not include specific cybersecurity requirements for the Integrated Base Defense Security System or RMF process and did not reference DoD or Air Force cybersecurity policies. The guidance also did not establish Program Management Office roles and responsibilities. Because of this, the program manager did not know his role and responsibility for the RMF process, or that support resources existed. The AFAA also reported that the program manager did not develop a process to verify that the acceptance memorandum for the Integrated Base Defense Security System's authority to operate was valid and that personnel completed cybersecurity reviews, testing, and annual assessments. Finally, the AFAA reported that 78th Security Forces Squadron personnel received training related to their job descriptions, but that training did not address RMF implementation and monitoring cybersecurity controls.

(U) The AFAA concluded that by maintaining a current authority to operate, officials could validate the Integrated Base Defense Security System's security posture and baseline configuration, and verify up-to-date security controls and patching were in place for the system.

(U) The AFAA made five recommendations concerning the improvements to the Integrated Base Defense Security System RMF process, including for the 78th Security Forces Squadron Commander to develop a standard operating procedure for continuously monitoring RMF implementation. As of August 2022, four recommendations were closed, and one was resolved and remained open.

(U) Data Security Category

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Government Accountability Office Report No. GAO-21-288, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 24, 2021

(U) The GAO performed a study on the Government's progress, including that of the DoD, for establishing a comprehensive cybersecurity strategy and performing effective oversight, securing its systems and information, protecting cyber critical infrastructure, and protecting privacy and sensitive data.

(U) The GAO determined that, although Government agencies made improvements in addressing recommendations for major cybersecurity challenges identified by the GAO in 2018, they had not implemented about 50 of the 80 recommendations the GAO made to enhance infrastructure cybersecurity. The GAO reported that Government agencies should move with greater urgency commensurate with rapidly evolving and grave threats to the country in improving infrastructure cybersecurity. In addition, the GAO determined that the National Security Strategy and implementation plan addressed some, but not all, of the desirable characteristics of national strategies, such as goals and resources needed. Furthermore, the GAO determined that the Government made progress in securing its systems and information, but continued to have numerous cybersecurity weaknesses resulting from ineffective information security programs. The GAO identified that the DoD had identified steps to improve its cyber hygiene, but did not know

(U) to what extent those steps were implemented. Lastly, the GAO determined that the Government did not have a comprehensive Internet privacy law governing the collection, use, and sale or other disclosure of personal information.

(U) The GAO concluded that if the Government did not implement the GAO's recommendations and act to address the four cybersecurity challenges identified in its 2018 report, the Government's IT systems, the Nation's critical infrastructure, and the personal information of U.S. citizens would be more susceptible to cybersecurity-related threats.

(U) The GAO did not make recommendations in this report.

(U) Information Protection Processes and Procedures Category

(U) Air Force Audit Agency Report No. F2022-0009-O10000, "Ports, Protocols, and Services Management," May 11, 2022

(U) The AFAA determined that Air Combat Command/Cyberspace Capabilities Center officials did not remove 33 percent of expired system registrations from the Ports, Protocols, and Services Management Registry in accordance with DoD policy. In addition, the AFAA determined that Cyberspace Capabilities Center officials did not register 152 information systems in the Management Registry, resulting in 62 percent of the ports being misconfigured.

(U) The AFAA reported that the Air Force CIO and Cyberspace Capabilities Center did not monitor and provide periodic oversight of the Management Registry to ensure it was updated; establish a notification process to inform system administrators of expired system registrations; or issue guidance addressing ports, protocols, and services implementation.

(U) The AFAA concluded that managing ports, protocols, and services in accordance with DoD policy enables the Air Force to protect its systems from cyber threats and enhances operational reliability and data integrity critical to mission execution.

(U) The AFAA made two recommendations to improve ports, protocols, and services management, including for the Commander of the Air Combat Command to direct Cyberspace Capabilities Center officials to include the 152 unregistered systems in the Management Registry and review expired system registrations to determine whether they should be renewed or removed. As of August 2022, one recommendation was closed, and one was resolved and remained open.

(U) Air Force Audit Agency Report No. F2020-0041-REO000, "Integrated Base Defense Security System Risk Management Framework 181st Intelligence Wing, Air National Guard, Hulman Field ANGB, IN," September 17, 2020

(U) The AFAA determined that 181st Intelligence Wing officials did not comply with RMF requirements to obtain an authority to operate or maintain required RMF documentation for the Integrated Base Defense Security System.

(U) The AFAA reported that conflicting Air Force guidance resulted in noncompliance with RMF requirements.

(U) The AFAA concluded that successfully implementing the RMF process enhanced the operational reliability and integrity of system security, which was vital to protecting critical Air Force infrastructure from physical and cybersecurity risks.

(U) The AFAA made two recommendations concerning improvements to meet RMF requirements, including for the 181st Intelligence Wing Commander to ensure that squadron officials develop and implement RMF cybersecurity training requirements for officials responsible for managing system security. As of August 2022, both recommendations were resolved and remained open.

(U) Maintenance Category

(U) Air Force Audit Agency Report No. F2021-0006-RWP000, "Wireless Network 374th Air Wing Yokota Air Base, Japan," January 4, 2021

(U) The AFAA determined that 374th Communications Squadron officials did not take actions to manage wireless network security. Specifically, the AFAA identified that officials did not identify or perform touch maintenance on inoperable access points on the Aruba AirWave Management System or conduct site surveys, referred to as "wardriving," to determine the wireless network's vulnerability to intrusion.

(U) The AFAA reported that the Base Information Transport Infrastructure Program Management Office did not develop a standard repeatable security process or properly train installation-level communications officials on conducting continuous monitoring.

(U) The AFAA concluded that ineffective wireless network security management could allow unauthorized access to Air Force networks or sensitive information, or allow malicious actors to commit fraud, launch attacks, or disrupt Air Force operations.

(U) The AFAA made two recommendations to improve wireless network security, including for the 374th Air Wing Commander to direct 374th Communications Squadron personnel to perform touch maintenance and restore functionality to the two inoperable wireless access points identified during the audit. These recommendations are closed.

(U) Protective Technology Category

(U) DoD Office of Inspector General Report No. DODIG-2022-061, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors," February 22, 2022

(U) The DoD OIG determined that ten assessed academic and research contractors did not consistently implement required cybersecurity controls to protect CUI on their networks from internal and external cyber threats. Specifically, the DoD OIG identified that:

- (U) four contractors did not enforce the use of multifactor authentication or configure their systems to enforce the use of strong passwords to access their networks and systems;
- (U) three contractors did not identify and mitigate network and system vulnerabilities in a timely manner;
- (U) one contractor did not monitor network traffic and scan its network for viruses;
- (U) two contractors did not encrypt workstation hard drives to protect CUI from unauthorized access or disclosure;
- (U) four contractors did not disable users' accounts after extended periods of inactivity;
- (U) five contractors did not protect CUI stored on removable media by using automated controls to restrict the use of removable media; and
- (U) one contractor did not develop an incident response plan.

(U) The DoD OIG reported that DoD Component contracting officers did not verify whether contractors complied with NIST Special Publication 800-171 cybersecurity requirements.[27]

(U) The DoD OIG concluded that academic and research contractors not fully implementing security controls in NIST Special Publication 800-171 and DoD Component contracting officers not monitoring compliance with these controls increased risk that academic and research contractors performing work for the DoD could become victims of cyberattacks.

[27] (U) NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," February 2020.

(U) The DoD OIG made 10 recommendations concerning improving controls to protect CUI, including for the Commander of the Naval Sea Systems Command to ensure contracting officers verified that contractors implemented technical security controls to protect CUI stored on removable media. As of August 2022, four recommendations were closed, and of the remaining six open recommendations, one was unresolved and five were resolved.

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Detect Function

(U) We determined there were 24 unclassified and classified reports and one testimony that identified risks regarding the Detect function. The Detect function includes activities that help organizations develop and implement appropriate activities to identify a cybersecurity event. The reports identified risks and weaknesses regarding the Detect function, such as organizations failing to monitor information systems and assets, that limit the DoD's ability to manage cybersecurity risks. Table 6 provides the NIST Cybersecurity Framework categories under the Detect function, the corresponding cybersecurity outcomes, and the number of reports and testimonies per category.

(U) Table 6. NIST Cybersecurity Framework Categories for the Detect Function

(U) Category	Cybersecurity Outcomes	Number of Reports	Number of Testimonies
Anomalies and Events	Organizations detect anomalous activity and understand the potential impact of events.	0	0
Security Continuous Monitoring	Organizations monitor information systems and assets to identify cybersecurity events and verify the effectiveness of protective measures.	21	1
Detection Processes	Organizations maintain and test detection processes and procedures to ensure awareness of anomalous events.	3	0 **(U)**

(U) Note: Totals may not equal the number of reports or testimonies identified because one may cover more than one NIST Cybersecurity Framework function.

(U) Source: NIST Cybersecurity Framework.

(U) The following sections provide examples of cybersecurity risks from the unclassified reports pertaining to the Detect function. For each category, we summarize examples of related reports' findings, causes, effects, and recommendations.

(U) Security Continuous Monitoring Category

(U) Air Force Audit Agency Report No. F2022-0013-REE000, "Cybersecurity of Automatic Test Systems and Equipment, 48th Fighter Wing, Royal Air Force Lakenheath, United Kingdom," April 18, 2022

> (U) The AFAA determined that 48th Maintenance Group officials did not assess automatic test systems and equipment for cybersecurity vulnerabilities throughout the devices' life cycles. Specifically, the AFAA identified that maintenance officials did not complete required updates or scan external media for viruses or malicious software.

(U) The AFAA reported that maintenance officials did not develop a process to scan external media or receive clear guidance on how often to install required updates.

(U) The AFAA concluded that effective cyber hygiene mitigated weapon system vulnerabilities and enhanced network security, enabling Air Force officials to reduce network risk.

(U) The AFAA made four recommendations concerning improving cybersecurity practices for test systems and equipment, including for the 48th Maintenance Group Commander to establish a process to scan external media before inserting it into a device. As of August 2022, all recommendations were resolved and remained open.

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Detection Processes Category

(U) Air Force Audit Agency Report No. F2021-0007-O10000, "Wireless Network," September 23, 2021

> (U) The AFAA determined that Air Force officials did not manage wireless network security and network requirements or account for assets effectively. Specifically, the AFAA identified that officials did not complete security assessments and continuously monitor the Base Information Transport Infrastructure wireless network or account for 72 percent of access points in a system of record at 10 of the 14 locations reviewed. In addition, the AFAA identified that Air Force officials did not manage wireless network requirements at any of the 14 locations reviewed.
>
> (U) The AFAA reported that Air Force officials did not implement adequate guidance and training.
>
> (U) The AFAA concluded that completing security assessments and performing continuous monitoring for the Base Information Transport Infrastructure wireless network identified security weaknesses, enabled immediate mitigation, and denied adversaries network access. The AFAA also concluded that accounting for access points reduced the risk of fraud, waste, and theft, and helped ensure device security was up to date. Furthermore, the AFAA concluded that managing wireless network requirements reduced unnecessary infrastructure, eliminated redundant capabilities, and ultimately reduced costs.
>
> (U) The AFAA made eight recommendations to improve wireless network management, including for the Director of the Air Combat Command Directorate of Cyberspace and Information Dominance to train officials to use monitoring capabilities and discontinue modernizing unused access points. As of August 2022, one recommendation was closed, and the remaining seven were resolved and remained open.

(U) Respond Function

(U) We determined there were 10 unclassified and classified reports, and one testimony that identified cybersecurity risks regarding the Respond function. The Respond function includes activities that demonstrate the development and implementation of appropriate activities to take action when detecting a cybersecurity incident. The reports identified risks and weaknesses regarding the Respond function, such as failures to coordinate response activities with internal and external stakeholders, that limit the DoD's ability to manage cybersecurity risks. Table 7 provides the NIST Cybersecurity Framework categories under the Respond function, the corresponding cybersecurity outcomes, and the number of reports and testimonies per category.

(U) Table 7. NIST Cybersecurity Framework Categories for the Respond Function

(U) Category	Cybersecurity Outcomes	Number of Reports	Number of Testimonies
Response Planning	Organizations execute and maintain response processes and procedures to respond to detected cybersecurity incidents.	2	0
Communications	Organizations coordinate response activities with internal and external stakeholders, such as external support from law enforcement agencies.	6	0
Analysis	Organizations conduct analysis to ensure effective response and support recovery activities.	1	0
Mitigation	Organizations perform activities to contain a cybersecurity event, mitigate its effects, and resolve the incident.	2	0
Improvements	Organizations improve response activities by incorporating lessons learned from current and previous detection and response activities.	2	1 **(U)**

(U) Note: Totals may not equal the number of reports or testimonies identified because one may cover more than one NIST Cybersecurity Framework function.

(U) Source: NIST Cybersecurity Framework.

(U) The following sections provide examples of cybersecurity risks from unclassified reports pertaining to the Respond function. For each category, we summarize examples of related reports' findings, causes, effects, and recommendations.

(U) Response Planning Category

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Communications Category

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Air Force Audit Agency Report No. F2021-0002-O10000, "Agreed-Upon Procedures, Personnel Budget and Analysis System Web – Test of Design and Effectiveness," March 26, 2021

(U) The AFAA determined during an agreed-upon procedures engagement that the Air Force had policies and procedures for identifying and responding to security violations for the Personnel Budget and Analysis System Web. Specifically, the AFAA determined those policies and procedures included reviewing system logs to monitor user account activities, responsibility for reviewing system logs, and how frequently system logs should be reviewed. The AFAA tested the Personnel Budget and Analysis System Web procedures and determined that Air Force officials were conducting system log reviews, identifying violations, and taking corrective actions in accordance with the established policy.

(U) The AFAA did not make recommendations in this report.

(U) Analysis Category

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Mitigation Category

(U) Air Force Audit Agency Report No. F2021-0004-O10000, "Air Force Data Vault," May 10, 2021

(U) The AFAA determined that Air Force Data Visible, Accessible, Understandable, Linked, and Trusted (VAULT) platform officials did not properly implement the RMF process to reduce cybersecurity risk by categorizing, assessing, and authorizing the system to protect its data. Specifically, VAULT officials did not update system information types, properly document security controls penetration testing results, or remedy or justify issues found during penetration testing in the required timeframe.

(U) The AFAA reported a lack of processes and oversight of the RMF process, and noncompliance with guidance. For example, the AFAA identified that noncompliance occurred despite VAULT officials' awareness of and training on RMF requirements. Also, the AFAA identified that VAULT officials did not establish a process to maintain an updated inventory of all types of information transported, stored, and processed through VAULT to support categorization requirements. Furthermore, the AFAA identified that the VAULT program manager did not verify officials completed RMF requirements.

(U) The AFAA concluded that completing required RMF processes helps VAULT officials reduce cybersecurity risk to the confidentiality, integrity, and availability of VAULT data and provides the foundation for technical control selection and continuous risk monitoring.

(U) The AFAA made two recommendations concerning reducing cybersecurity risks, including for the Air Force Chief Data Officer to require VAULT officials to post security authorization documents in the enterprise Mission Assurance Support Service and complete all RMF requirements. These recommendations are closed.

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(~~CUI~~) [redacted]

(U) Improvements Category

(U) Government Accountability Office Report No. GAO-22-104746, "Cybersecurity, Federal Response to SolarWinds and Microsoft Exchange Incidents," January 13, 2022

(U) The GAO determined that Federal agencies took action to coordinate and respond to the SolarWinds and Microsoft Exchange incidents. For example, the GAO determined that two Cyber Unified Coordination Groups coordinated the Government-wide response to the SolarWinds and Microsoft Exchange incidents, respectively. The GAO identified that Cyber Unified Coordination Group efforts included issuing directives, guidance, advisories, alerts, and tools to agencies.

(U) The GAO also determined that Federal agencies reported the actions they took to mitigate the threats introduced by the SolarWinds and Microsoft Exchange incidents as well as additional information regarding network activity and each incident's impact on the Department of Homeland Security Cybersecurity and Infrastructure Security Agency.

(U) In addition, the GAO determined that Federal agencies identified practices that officials believed aided and hindered responses to the SolarWinds and Microsoft Exchange incidents. For example, the GAO identified that Cyber Unified Coordination Groups officials reported that information sharing with the private sector allowed the Government to identify the scale of the SolarWinds incident and respond quickly. The GAO also identified that Cyber Unified Coordination Groups officials reported that information sharing provided increased visibility on the status of patching and the extent of the vulnerabilities and exploitation in the case of Microsoft Exchange.

(U) The GAO also identified that Federal agencies reported difficulties in responding to the SolarWinds and Microsoft Exchange incidents, including varying levels of classification and the lack of an agreed-upon method for sharing information.

(U) The GAO did not make recommendations in this report.

(U) Recover Function

(U) We determined that there was one unclassified report that identified risks regarding the Recover function. The Recover function includes activities that support timely recovery of normal operations to reduce the impact from a cybersecurity incident. The report identified failures to complete corrective actions regarding the Recover function that limit the DoD's ability to manage cybersecurity risks. Table 8 provides the NIST Cybersecurity Framework categories under the Recover function, the corresponding cybersecurity outcomes, and the number of reports and testimonies per category.

(U) Table 8. NIST Cybersecurity Framework Categories for the Recover Function

(U) Category	Cybersecurity Outcomes	Number of Reports	Number of Testimonies
Recovery Planning	Organizations execute and maintain recovery processes and procedures to restore systems or assets affected by cybersecurity incidents.	0	0
Improvements	Organizations improve recovery planning and processes by incorporating lessons learned into future activities.	1	0
Communications	Organizations coordinate restoration activities with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, and vendors.	0	0 (U)

(U) Note: Totals may not equal the number of reports or testimonies identified because one may cover more than one NIST Cybersecurity Framework function.

(U) Source: NIST Cybersecurity Framework.

(U) The following section provides an example of cybersecurity risks from the unclassified report pertaining to the Recover function. We summarize the related report's findings, causes, effects, and recommendations.

(U) Improvements Category

(U) Air Force Audit Agency Report No. F2021-0005-O20000, "Electronic Records Cyber Hygiene," August 17, 2021

> (U) The AFAA determined that Air Force officials completed corrective actions to address recommendations the AFAA made in F2018-0005-O10000, "Electronic Records Cyber Hygiene," December 27, 2017. Specifically, the AFAA identified that Air Force officials implemented effective backup procedures, and developed and tested contingency plans.
>
> (U) The AFAA did not make recommendations in this report.

(U) Open Cybersecurity-Related Recommendations

(U) We are not making new recommendations to DoD management in this summary report, but it is vital to the DoD's overall cybersecurity posture that management implement comprehensive corrective actions in a timely manner to address the open recommendations. When considering open recommendations, we also included IT NFRs, which independent public accounting firms issue to communicate internal control deficiencies to management. We determined that as of June 30, 2022, the DoD needed to take action to close 478 open DoD cybersecurity-related recommendations—317 unclassified and 161 classified—from reports dating as far back as FY 2012. The 478 open cybersecurity-related recommendations have remained open for an average of 364 days when factoring in open recommendations from FY 2012. 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.

(U) The DoD OIG and GAO made 8 cybersecurity-related recommendations before July 2017 that remained open as of June 2022, with the oldest dating back to August 2012. By not taking timely corrective action, the DoD could compromise its overall cybersecurity posture.

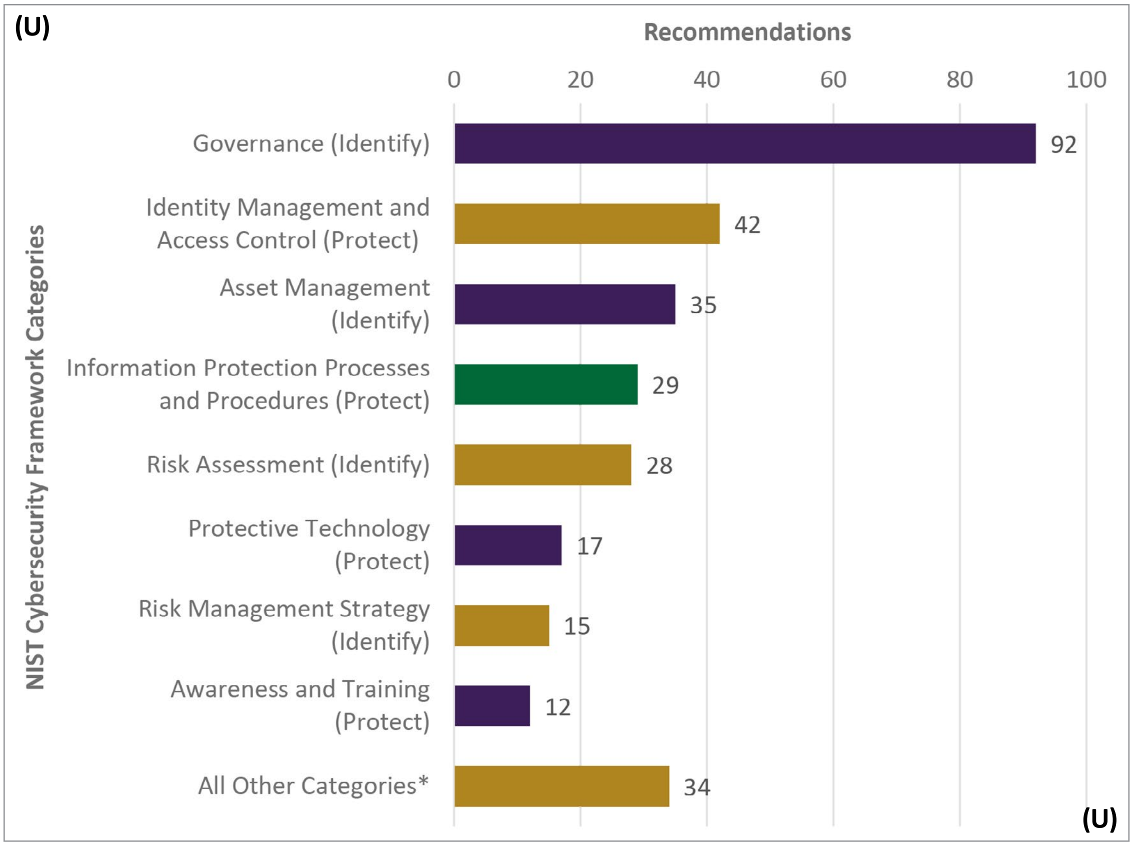
- (U) The DoD OIG made 7 recommendations, including to:
  - (U) establish a working group to develop and implement additional functionality into the General Fund Enterprise Business System that enables the Army to generate an Army-wide real property universe;

  - (U) review control weaknesses identified for the Defense Cash Accountability System and Program Budget Information System during Federal Information System Controls Audit Manual testing and implement a plan to reduce ineffective or untested controls; and
  - (U) limit the permissions of specific users of the Navy Enterprise Resource Planning system so the users only have the permissions necessary to perform their duties.
- (U) The GAO made one recommendation to define the Senior Information Security Officer's role in DoD policy for ensuring that the DoD had procedures for detecting, responding, and reporting incidents.

(U) Status of Recommendations from Reports Issued from July 1, 2020, Through June 30, 2022

(U) The DoD OIG, GAO, and other DoD oversight organizations made 438 cybersecurity-related recommendations to the DoD from July 1, 2020, through June 30, 2022. Of these, 291 recommendations—212 unclassified and 79 classified—remained open as of June 30, 2022, with the majority pertaining to the Identify and Protect functions. The 291 open cybersecurity-related recommendations issued since July 1, 2020, have remained open for an average of 279 days. Figure 3 shows open DoD cybersecurity-related recommendations, by NIST Cybersecurity Framework category, from reports included in this summary.

(U) Figure 3. Open Unclassified and Classified DoD Cybersecurity-Related Recommendations by NIST Cybersecurity Framework Category from July 1, 2020, through June 30, 2022



* (U) The "All Other Categories" column comprises the remaining 15 of the 23 NIST Cybersecurity Framework categories.

(U) Note: Totals may not equal the number of recommendations identified because one recommendation may apply to more than one NIST Cybersecurity Framework category.

(U) Source: The DoD OIG.

(U) As of June 30, 2022, DoD management agreed with 267 of the 291 open cybersecurity-related recommendations; however, the remaining 24 recommendations are unresolved. DoD management either did not respond, partially agreed, or disagreed with these 24 recommendations.

(U) Status of Open Information Technology Notices of Findings and Recommendations as of July 15, 2022

(U) Auditors and the DoD OIG issued 1,417 IT NFRs related to the FY 2021 financial statement audits and attestations of 26 DoD reporting entities. IT NFRs communicate to management any identified IT system internal control deficiencies affecting financial processes, their causes, and how to correct them.[28] Of the 1,417 IT NFRs, 1,304, or 92 percent, remained open as of July 15, 2022. New IT NFRs represent issues first identified during the current year's audit; reissued IT NFRs represent issues identified during a prior audit that remain uncorrected. Table 9 shows the distribution and status—new or reissued—of open IT NFRs among the DoD reporting entities.

(U) Table 9. Distribution of Open IT NFRs Among DoD Reporting Entities

(U) DoD Reporting Entity	Open IT NFR Count (As of July 15, 2022)	New IT NFRs	Reissued IT NFRs
Department of the Navy	495	26	469
Department of the Air Force	246	64	182
Department of the Army	142	60	82
Other DoD Reporting Entities	119	40	79
U.S. Marine Corps	102	102	0
Defense Logistics Agency	54	18	36
U.S. Special Operations Command	46	20	26
U.S. Transportation Command	42	0	42
Defense Information Systems Agency	17	12	5
Medicare Eligible Retiree Health Care Fund	12	2	10
Defense Health Agency – Contract Resource Management	11	1	10
U.S. Army Corps of Engineers	8	5	3
Military Retirement Fund	8	3	5
Agency-Wide	2	1	1
Total	**1,304**	**354**	**950** **(U)**

(U) Source: The DoD OIG.

[28] (U) DoD OIG Report, "Understanding the Results of the Audit of the FY 2021 DoD Financial Statements," May 18, 2022.

(U) We selected a nonstatistical sample of 44 of the 1,304 open IT NFRs and determined that the IT NFRs identified cybersecurity risks as described in the NIST Cybersecurity Framework.[29] We reviewed and categorized these 44 open IT NFRs based on the NIST Cybersecurity Framework. We categorized the 44 IT NFRs as follows:

- (U) 21 included risks regarding the Identity Management, Authentication and Access Control category (Protect function);
- (U) 16 included risks regarding the Governance category (Identify function);
- (U) 7 included risks regarding the Information Protection Processes and Procedures category (Protect function);
- (U) 5 included risks regarding the Protective Technology category (Protect function);
- (U) 3 included risks regarding the Asset Management category (Identify function);
- (U) 3 included risks regarding the Anomalies and Events category (Detect function);
- (U) 2 included risks regarding the Analysis category (Respond function);
- (U) 1 included risks regarding the Business Environment category (Identify function);
- (U) 1 included risks regarding the Data Security category (Protect function); and
- (U) 1 included risks regarding the Mitigation category (Respond function).[30]

(U) The following sections provide examples from the 44 IT NFRs that identified weaknesses regarding the Identity Management, Authentication, and Access Control and Governance categories. For each example, we summarize the findings, cause, effect, and recommendations.

[29] (U) According to the Council of the Inspectors General on Integrity and Efficiency *Journal of Public Inquiry, Fall/Winter 2012-2013*, "a sample size should be 44 if the total population is between 501 and 2,000."

[30] (U) Totals may not equal the number of IT NFRs identified because one IT NFR may cover more than one NIST Cybersecurity Framework category.

(U) Identity Management, Authentication, and Access Control Category (Protect Function)

(U) We determined that 21 of the 44 NFRs we reviewed identified weaknesses regarding the Identity Management, Authentication, and Access Control category. Specifically, 14 of the 21 NFRs included risks regarding implementing the principle of least privilege.[31]

(U) For example, the auditors determined that the Navy's Simplified Workflow Access Protocol tool allowed Standard Accounting and Reporting System users to designate the supervisor approving their access to the application without validating the appropriateness of the assignments. The auditors reported that there was no process in place to confirm that prospective users selected the correct supervisor during the account approval process. The auditors concluded that without an automated process or mitigating controls for assigning the appropriate supervisors to access requests, the system has a critical risk of inappropriately approving access. The auditors also concluded that the lack of an automated and monitored process could provide a user with unauthorized access to the system, risking the system's confidentiality, integrity, and availability of the data used for financial reporting-related activities.

(U) The auditors recommended that Standard Accounting and Reporting System management develop a process to confirm the appropriateness of the user's supervisor when approving access to new system users.

(U) Governance (Identify Function)

(U) We determined that 16 of the 44 NFRs we reviewed identified weaknesses regarding the Governance category. Specifically, 15 of the 16 NFRs included risks regarding establishing and communicating organizational cybersecurity policies and procedures necessary for managing risk.

(U) For example, the auditors determined that Marine Corps Total Force System management did not implement procedures to completely resolve transaction level and file errors in a timely manner. The auditors reported that the error-handling framework was incomplete because it did not include procedures for tracking, reviewing, and remedying errors. The auditors concluded that the absence of certain procedures increased the risk of undetected errors, leading

[31] (U) According to NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," September 2020, Revision 5, the principle of least privilege states that each system component is allocated sufficient privileges to accomplish its specified functions but no more. Applying the principle of least privilege limits the scope of the component's actions, which has two desirable effects: the security impact of a failure, corruption, or misuse of the component will have a minimized security impact, and the security analysis of the component will be simplified.

(U) to a negative impact on the accuracy and integrity of the data processed via the system. The auditors recommended that the Marine Corps establish requirements defining the specific remediation timelines for addressing errors and disseminate updated procedures to verify that identified errors were reviewed and remedied consistently and in a timely manner.

(U) Trends from Information Technology NFRs

(U) From FY 2018 through FY 2021, auditors issued or reissued 1,417 IT NFRs to address internal control weaknesses and deficiencies. Table 10 shows the number of IT NFRs issued each fiscal year resulting from the FY 2018-2021 DoD financial statement audits.

(U) Table 10. IT NFRs Issued Related to FY 2018 – FY 2021 DoD Financial Statement Audits

(U) Fiscal Year	New IT NFRs	Reissued IT NFRs	Total
2018	1,208	99	1,307
2019	836	858	1,694
2020	523	1,150	1,673
2021	362	1,055	1,417 **(U)**

(U) Note: NFRs are associated with each fiscal year's financial statement audits. As of June 30, 2022, only the FY 2021 NFRs are current. NFRs from FY 2018 through FY 2020 are included for comparison.

(U) Source: The DoD OIG.

(U) The total number of IT NFRs decreased from 1,673 in FY 2020 to 1,417 in FY 2021 (15 percent) while the number of reissued IT NFRs also decreased from 1,150 in FY 2020 to 1,055 in FY 2021 (8 percent). The reduction in IT NFRs represents a decrease in internal control weaknesses and deficiencies identified during the audits. However, the DoD OIG reported in May 2022 that the number of material weaknesses remained constant between FY 2020 and FY 2021 despite the DoD's efforts to prioritize the remediation of IT material weaknesses.[32]

(U) We determined that these IT material weaknesses aligned with the following NIST Cybersecurity Framework functions and categories.

- (U) DoD Components lacked effective configuration and security management controls - Information Protection Processes and Procedures category (Protect function)

[32] (U) DoD OIG Report, "Understanding the Results of the Audit of the FY 2021 DoD Financial Statements," May 18, 2022.

- (U) DoD Components did not perform comprehensive periodic reviews of all users with access to key information systems to validate whether user access aligned with their roles and responsibilities - Identity Management Authentication and Access Control category (Protect function)
- (U) DoD Components did not develop processes to properly identify conflicting roles or segregate key functions - Identity Management Authentication and Access Control category (Protect function)
- (U) DoD management did not consider compliance with Federal system requirements when defining legacy systems, and therefore, did not properly classify at least 140 systems as legacy systems - Asset Management category (Identify function)

(U) Ineffective IT system controls and business practices identified in NFRs leave the DoD at risk of continuing to produce financial statements that are unreliable. A lack of effective system controls could result in significant risk to DoD assets. For example, payments and collections could be lost, stolen, or duplicated. The DoD can improve understanding of and address internal control deficiencies by implementing recommended actions included in the IT NFRs.

(U) Opportunity Exists to Improve Cybersecurity Oversight

(U) The DoD OIG, GAO, and other DoD oversight organizations' reports, recommendations, and testimonies primarily focused on two of the five NIST Cybersecurity Framework functions—Identify and Protect, which focus on understanding how to manage cybersecurity risk and developing and implementing appropriate safeguards. The remaining three functions, Detect, Respond, and Recover, focus on identifying cybersecurity events, taking actions to contain those events, and restoring capabilities or services impaired.

(U) According to NIST, organizations should perform tasks associated with all functions concurrently and continuously to form a culture that addresses dynamic cybersecurity risks. There was less oversight provided by the DoD OIG, GAO, and the other DoD oversight organizations of three NIST Cybersecurity Framework functions—Detect, Respond, and Recover. The DoD OIG continues to identify cybersecurity-related risks as a major challenge facing the DoD, and has included it in its Top DoD Management Challenges report for the past five years. Strategically increasing oversight of under-assessed areas will provide the DoD increased assurance that its actions taken in relation to these three Framework functions are effective and operating as intended.

(U) Appendix A

(U) Scope and Methodology

(U) We conducted this summary work from December 2021 through December 2022 in accordance with generally accepted government auditing standards, except for the standards of planning and evidence because this report summarizes previously released reports.

(U) This report summarizes unclassified reports issued by the DoD OIG, GAO, and the other DoD oversight organizations from July 1, 2020, through June 30, 2022. Because the issues identified in the classified reports were similar to the issues included in the unclassified summary, we did not issue separate classified appendixes summarizing that information. Instead, we included summary-level information in the figures and tables pertaining to the number of classified reports and number of recommendations. To prepare this summary, we coordinated with members of the DoD audit community, the DoD Intelligence Community agencies, and the GAO to obtain unclassified reports and classified reports (up to TOP SECRET). We reviewed information reported by the DoD oversight organizations, including summary information reported by the DoD Intelligence Community agencies and we categorized that information 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 cybersecurity reports, testimonies, or other oversight information provided. Additionally, because many of the summarized reports contained recommendations regarding the identified cybersecurity risks, we do not make recommendations in this summary report.

(U) This report also summarizes DoD IT NFRs. To prepare this summary, we coordinated with the DoD OIG Quantitative Methods Division to develop a nonstatistical sample of IT NFRs.[33] As of July 15, 2022, the DoD had 1,304 open IT NFRs. Based on this population of open IT NFRs, we selected a nonstatistical sample of 44 open IT NFRs to categorize the findings based on the NIST Cybersecurity Framework, and we provided a summary of the NFRs' findings as they pertain to the NIST Cybersecurity Framework.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any

[33] (U) 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.

(U) comments submitted by the DoD Component about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

(U) Use of Computer-Processed Data

(U) We obtained the total universe of DoD open IT NFRs from the DoD Office of the Deputy Chief Financial Officer NFR Database as of July 15, 2022. The NFR 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 IT NFRs obtained from the NFR Database was sufficient and reliable to support the NFRs' findings as they pertain to the NIST Cybersecurity Framework.

(U) Prior Coverage

(U) During the last 5 years, the DoD OIG issued 4 reports that summarized 143 DoD cybersecurity-related reports—115 unclassified and 28 classified—and 4 unclassified testimonies made by the DoD OIG, GAO, and the other DoD oversight organizations.

(U) The publicly released DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/. Legacy For Official Use Only (FOUO) or CUI reports can be requested by filing a Freedom of Information Act request online at http://www.dodig.mil/FOIA/Submit-FOIA.

(U) DoD OIG

(U) Report No. DODIG-2021-034, "Summary of Reports and Testimonies Regarding DoD Cybersecurity From July 1, 2019, Through June 30, 2020," December 11, 2020 (Report is CUI)

> (U) The DoD OIG identified 44 DoD cybersecurity-related reports—33 unclassified and 11 classified—issued by the DoD OIG, GAO, and other DoD oversight organizations from July 1, 2019, through June 30, 2020. The DoD OIG determined that the DoD Components implemented improvements regarding the NIST Cybersecurity Framework categories. However, the DoD identified that the DoD continued to face significant challenges in managing cybersecurity risks to its systems and networks. As of August 2020 the DoD had 459 cybersecurity-related recommendations open, dating back as far as 2011.

(U) 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)

> (U) The DoD OIG identified 46 DoD cybersecurity-related reports—33 unclassified and 13 classified—and three testimonies provided to Congress by the DoD OIG, GAO, and other DoD oversight organizations from July 1, 2018, through June 30, 2019. The DoD OIG determined that the DoD Components implemented corrective actions necessary to mitigate or remedy risks and weaknesses to DoD systems and networks identified in this summary report and prior summary reports. 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.

(U) 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)

> (U) 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, relating to 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.

(U) 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)

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

(U) Appendix B

(U) Unclassified and Classified Reports and Testimonies Regarding DoD Cybersecurity

(U) Reports

(U) GAO

1. (U) Report No. GAO-22-105834, "Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance," March 30, 2022
2. (U) Report No. GAO-22-104560, "Cybersecurity: Internet Architecture is Considered Resilient, but Federal Agencies Continue to Address Risks," March 3, 2022
3. (U) Report No. GAO-22-104765, "Artificial Intelligence: Status of Developing and Acquiring Capabilities for Weapon Systems," February 17, 2022
4. (U) Report No. GAO-22-104746, "Federal Response to SolarWinds and Microsoft Exchange Incident," January 13, 2022
5. (U) Report No. GAO-22-104679, "Stakeholder Communication and Performance Goals Could Improve Certification Framework," December 8, 2021
6. (U) Report No. GAO-22-105530, "Federal Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure," December 2, 2021
7. (U) Report No. GAO-22-104422, "Quantum Computing and Communications Status and Prospects," October 19, 2021
8. (U) Report No. GAO-21-105283, "DOD Should Explore Options to Meet User Needs for Narrowband Capabilities," September 2, 2021
9. (~~CUI~~) [redacted]
10. (U) Report No. GAO-21-351, "DoD Faces Risks and Challenges in Implementing Modern Approaches and Addressing Cybersecurity Practices," June 23, 2021
11. (U) Report No. GAO-21-278, "Defense Logistics Agency Needs to Address Risk Management Deficiencies in Inventory Systems," June 21, 2021
12. (U) Report No. GAO-21-222, "Updated Program Oversight Approach Needed," June 8, 2021

13. (U) Report No. GAO-21-279, "Department of Defense Domain Readiness Varied from Fiscal Year 2017 Through Fiscal Year 2019," April 7, 2021
14. (U) Report No. GAO-21-288, "Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges," March 24, 2021
15. (U) Report No. GAO-21-256SU, "Actions Need to Address 5G Telecommunications Risks," March 5, 2021
16. (U) Report No. GAO-21-179, "Guidance Would Help DoD Programs Better Communicate Requirements to Contractors," March 4, 2021
17. (U) Report No. GAO-21-158, "Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed," January 12, 2021
18. (U) Report No. GAO-21-182, "DoD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule," December 23, 2020
19. (U) Report No. GAO-21-68, "Joint Cyber Warfighting Architecture Would Benefit from Defined Goals and Governance," November 19, 2020
20. (U) Report No. GAO-20-252, "DoD Needs to Implement Comprehensive Plans to Improve Its Systems Environment," September 30, 2020
21. (U) Report No. GAO-20-13C , "DoD Has Authorities and Organizations in Place, but Policies, Processes, and Reporting Could be Improved," September 28, 2020 (Report is SECRET)
22. (U) Report No. GAO-20-629, "Clarity of Leadership Urgently Needed to Fully Implement the National Strategy," September 22, 2020
23. (U) Report No. GAO-20-249SP, "Key Attributes of Essential Federal Mission-Critical Acquisitions," September 8, 2020

(U) DoD OIG

24. (U) Report No. DoDIG-2022-092, "Management Advisory on DoD's Compliance with the Cybersecurity Information Sharing Act of 2015," May 10, 2022
25. (U) Report No. DoDIG-2022-089, "Joint Audit of the Department of Defense and the Department of Veterans Affairs Efforts to Achieve Electronic Health Record System Interoperability," May 5, 2022
26. (U) Report No. DoDIG-2022-061, "Audit of the Protection of Military Research Information and Technologies Developed by Department of Defense Academic and Research Contractors," February 22, 2022
27. (U) Report No. DoDIG-2022-041, "Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process," December 3, 2021

28. (U) Report No. DoDIG-2021-131, “Audit of Department of Defense Middle Tier of Acquisition Rapid Prototyping and Rapid Fielding Programs,” September 28, 2021

29. (U) Report No. DoDIG-2021-125, “Evaluation of U.S. Special Operations Command’s Supply Chain Risk Management for the Security, Acquisition, and Delivery of Specialized Equipment,” September 14, 2021

30. (U) Report No. DoDIG-2021-110, “Audit of the Department of Defense Recruitment and Retention of the Civilian Cyber Workforce,” July 29, 2021

31. (U) Report No. DoDIG-2021-100, “Audit of the Department of Defense’s Implementation of the Memorandums Between the Department of Defense and the Department of Homeland Security Regarding Cybersecurity and Cyberspace Operations,” July 9, 2021

32. (U) Report No. DoDIG-2021-098, “Audit of the Cybersecurity of Department of Defense Additive Manufacturing Systems,” July 1, 2021 (Report is CUI)

33. (U) Report No. DoDIG-2021-065, “Evaluation of Access to Department of Defense Information Technology and Communications During the Coronavirus Disease–2019 Pandemic,” March 30, 2021

34. (U) Report No. DoDIG-2021-064, “Audit of Maintaining Cybersecurity in the Coronavirus Disease–2019 Telework Environment,” March 29, 2021

35. (U) Report No. DoDIG-2021-054, “Audit of Cybersecurity Controls Over the Air Force Satellite Control Network,” February 17, 2021 (Report is TOP SECRET)

36. (U) Report No. DoDIG-2021-050, “Audit of Contracts for DoD Information Technology Products and Services Procured by DoD Components in Response to the Coronavirus Disease–2019 Pandemic,” February 12, 2021

37. (U) Report No. DoDIG-2021-051, “Audit of Cybersecurity Requirements for Weapon Systems in the Operations and Support Phase of the Department of Defense Acquisition Life Cycle,” February 10, 2021

38. (U) Report No. DoDIG-2021-043, “Audit of Depot-Level Reparable Items at Tobyhanna Army Depot,” January 8, 2021

39. (U) Report No. DoDIG-2021-001, “Audit of the Solicitation, Award, and Administration of Washington Headquarters Services Contract and Task Orders for Office of Small Business Programs,” October 7, 2020

40. (U) Report No. DoDIG-2020-122, “Audit of the Supply Chain Risk Management for the Navy’s Nuclear Weapons Delivery System,” September 1, 2020 (Report is SECRET)

(U) Army Audit Agency

41. (U) Report No. A-2022-0042-AXZ, “Army Data Center Optimization,” April 14, 2022

42. (~~CUI~~) [redacted]
43. (U) Report No. A-2022-0033-IIZ, "Cloud Migration," March 14, 2022
44. (U) Report No. A-2022-0026-AXZ, "Protective Measures Over PII in Europe," February 1, 2022
45. (U) Report No. A-2022-0015-AXZ, "Portable Electronic Devices and Wireless Services Management," December 10, 2021
46. (~~CUI~~) [redacted]
47. (~~CUI~~) [redacted]
48. (~~CUI~~) [redacted]
49. (U) Report No. A-2021-0051-AXZ, "Information Technology Spend—Unfunded Requirements," June 1, 2021
50. (~~CUI~~) [redacted]
51. (U) Report No. A-2021-0044-AXZ, "Followup Audit of DoD Information Network Operations Tools," April 30, 2021
52. (U) Report No. A-2021-0038-AXZ, "Information Technology Spend—Investment Threshold and Equipment Accountability Policy," April 5, 2021
53. (U) Report No. A-2021-0031-AXZ, "Information Technology Spend—Miscellaneous Obligations," March 15, 2021
54. (U) Report No. A-2021-0028-AXZ, "Information Technology Spend—Reimbursable Orders," February 16, 2021
55. (~~CUI~~) [redacted]
56. (~~CUI~~) [redacted]

(U) Naval Audit Service

57. (~~CUI~~) [redacted]
58. (~~CUI~~) [redacted]

59. (~~CUI~~) [redacted]

60. (~~CUI~~) [redacted]

61. (~~CUI~~) [redacted]

62. (~~CUI~~) [redacted]

63. (~~CUI~~) [redacted]

64. (~~CUI~~) [redacted]

65. (~~CUI~~) [redacted]

66. (~~CUI~~) [redacted]

67. (~~CUI~~) [redacted]

(U) Air Force Audit Agency

68. (U) Report No. F2022-0012-RWP000, "Cybersecurity of Automatic Test Systems and Equipment 18th Wing Kadena Air Base, Japan," June 27, 2022

69. (U) Report No. F2022-0011-RWC000, "Cryptographic Asset Accountability 35th Combat Communications Squadron Tinker AFB, OK," June 24, 2022

70. (U) Report No. F2022-0017-REE000, "Information Technology Accountability 501st Combat Support Wing Royal Air Force Alconbury, UK," June 1, 2022

71. (U) Report No. F2022-0008-RES000, "Cybersecurity of Automatic Test Systems and Equipment 23d Wing Moody Air Force Base, GA," May 26, 2022 (Report is CUI)

72. (U) Report No. F2022-0024-REG000, "Cybersecurity of Automatic Test Systems and Equipment 96th Test Wing Eglin Air Force Base, FL," May 26, 2022 (Report is CUI)

73. (U) Report No. F2022-0009-O10000, "Ports, Protocols, and Services Management," May 11, 2022

74. (U) Report No. F2022-0010-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Security Assistance Management Information Systems - Test of Design and Effectiveness," May 11, 2022
75. (U) Report No. F2022-0013-REE000, "Cybersecurity of Automatic Test Systems and Equipment 48th Fighter Wing Royal Air Force Lakenheath, United Kingdom," April 18, 2022
76. (U) Report No. F2022-0008-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Financial Management Feeder Systems Controls - Reserve Travel System - Test of Design and Effectiveness," January 21, 2022
77. (U) Report No. F2022-0007-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Financial Management Feeder Systems Controls - Unit Training Assembly System-Web - Test of Design and Effectiveness," January 18, 2022
78. (U) Report No. F2022-0012-REG000, "Weapon System Cyber Hygiene 6th Air Refueling Wing MacDill Air Force Base, FL," January 14, 2022 (Report is CUI)
79. (U) Report No. F2022-0006-O10000, "Cross Domain Solutions," January 12, 2022
80. (U) Report No. F2022-0005-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Financial Management Feeder Systems Controls - Air Force Promotions System/Weighted Airmen Promotions System - Test of Design and Effectiveness," January 11, 2022
81. (U) Report No. F2022-0003-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Financial Management Feeder Systems Controls - Reliability, Availability, and Maintainability of Pods - Test of Design and Effectiveness," December 14, 2021
82. (U) Report No. F2022-0004-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Financial Management Feeder Systems Controls - Personnel Budget and Analysis System Web - Test of Design and Effectiveness," December 14, 2021
83. (U) Report No. F2022-0002-O10000, "Protection of Technical and Proprietary Data," December 1, 2021 (Report is CUI)
84. (~~CUI~~) [redacted]
85. (U) Report No. F2022-0001-RWI000, "Printer and Multifunction Device Cybersecurity 412th Test Wing Edwards AFB, CA," October 22, 2021 (Report is CUI)

86. (~~CUI~~) [redacted]

87. (U) Report No. F2022-0003-REG000, “Cybersecurity of Network Component Purchases 81st Training Wing Keesler AFB, MS,” October 18, 2021

88. (U) Report No. F2022-0002-REG000, “Printer and Multifunction Devices Cybersecurity 81st Training Wing Keesler AFB, MS,” October 15, 2021

89. (~~CUI~~) [redacted]

90. (~~CUI~~) [redacted]

91. (~~CUI~~) [redacted]

92. (U) Report No. F2021-0007-O10000, “Wireless Network,” September 23, 2021

93. (~~CUI~~) [redacted]

94. (~~CUI~~) [redacted]

95. (~~CUI~~) [redacted]

96. (~~CUI~~) [redacted]

97. (U) Report No. F2021-0010-O30000, “Cloud Computing Security,” September 9, 2021

98. (~~CUI~~) [redacted]

99. (U) Report No. F2021-0012-RWC000, “Printer and Multifunction Device Cybersecurity 72d Air Base Wing Tinker Air Force Base, OK,” August 18, 2021

100. (U) Report No. F2021-0005-O20000, "Electronic Records Cyber Hygiene," August 17, 2021

101. (U) Report No. F2021-0024-RWI000, "Printers and Multifunction Devices Cybersecurity 75th Air Base Wing Hill AFB, UT," August 12, 2021

102. (~~CUI~~) [redacted]

103. (U) Report No. F2021-0005-O10000, "Software Use," May 19, 2021 (Report is CUI)

104. (U) Report No. F2021-0004-O10000, "Air Force Data Vault," May 10, 2021

105. (~~CUI~~) [redacted]

106. (U) Report No. F2021-0004-O30000, "Joint Mission Planning System Access Controls," April 2, 2021

107. (U) Report No. F2021-0002-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Personnel Budget and Analysis System Web - Test of Design and Effectiveness," March 26, 2021

108. (~~CUI~~) [redacted]

109. (U) Report No. F2021-0006-RWT000, "Software Use 56th Fighter Wing Luke AFB, AZ," January 11, 2021

110. (U) Report No. F2021-0007-REA000, "Software Use 20th Fighter Wing Shaw AFB, SC," January 11, 2021

111. (U) Report No. F2021-0006-RWP000, "Wireless Network 374th Air Wing Yokota Air Base, Japan," January 4, 2021

112. (U) Report No. F2021-0008-REG000, "Integrated Base Defense Security System – Risk Management Framework 96th Test Wing Eglin AFB, FL," December 1, 2020

113. (U) Report No. F2021-0004-RES000, "Integrated Base Defense Security System Risk Management Framework 23d Wing Moody AFB, GA," November 5, 2020

114. (U) Report No. F2021-0002-RES000, "Integrated Base Defense Security System Risk Management Framework 78th Air Base Wing Robins AFB, GA," November 4, 2020

115. (U) Report No. F2021-0001-REN000, "Integrated Base Defense Security System Risk Management Framework 103d Airlift Wing Bradley Air National Guard Base, CT," October 1, 2020

116. (U) Report No. F2020-0043-REO000, "Integrated Base Defense Security System Risk Management Framework Michigan Combat Readiness Training Center Air National Guard Alpena, MI," September 28, 2020

117. (U) Report No. F2020-0041-REO000, "Integrated Base Defense Security System Risk Management Framework 181st Intelligence Wing Air National Guard Hulman Field ANGB, IN," September 17, 2020

118. (U) Report No. F2020-0010-A00900, "Nuclear Cyber Security," August 25, 2020 (Report is SECRET)

119. (U) Report No. F2020-0009-A00900, "Cyber Program Management," August 17, 2020 (Report is TOP SECRET//TK//NOFORN)

120. (U) Report No. F2020-0014-O10000, "Independent Auditor's Report on Applying Agreed-Upon Procedures, Unit Training Assembly Processing System Web – Test of Design and Effectiveness," August 13, 2020

121. (U) Report No. F2020-0021-RWP000, "Information Technology Equipment Government Purchase Card Usage 353d Special Operations Group Kadena Air Base, Japan," August 6, 2020

(U) Other DoD Agencies

122. (~~CUI~~) [redacted]

123. (~~CUI~~) [redacted]

124. (U) Office of the Inspector General of the Intelligence Community Report No. AUD-2021-002-U, "Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015," December 9, 2021

125. (~~CUI~~) [redacted]

126. (~~CUI~~) [redacted]

127. (~~CUI~~) [redacted]

128. (U) Defense Information Systems Agency OIG Report No. 21-IG31-007, "Cyber Excepted Service Pay Quick Look, " September 28, 2021

129. (~~CUI~~) [redacted]

130. (~~CUI~~) [redacted]

131. (~~CUI~~) [redacted]

132. (~~CUI~~) [redacted]

133. (U) National Reconnaissance Office OIG Report No. 2019-003A, "Audit of the Management of Industry Partner Access," August 28, 2020 (Report is TOP SECRET//TK//NOFORN)

(U) Testimonies

(U) GAO

1. (U) Testimony No. GAO-22-105530, "Cybersecurity: Federal Actions Urgently Needed to Better Protect the Nation's Critical Infrastructure," December 2, 2021

2. (U) Testimony No. GAO-21-525T, "Information Environment: DoD Operations Need Enhanced Leadership and Integration of Capabilities," April 30, 2021

3. (U) Testimony No. GAO-21-440T, "Electromagnetic Spectrum: Operations DoD Needs to Take Action to Help Ensure Superiority," March 19, 2021

(U) Other DoD Agencies

4. (U) "Securing the Digital Commons: Open-Source Software Cybersecurity," Office of the Secretary of the Air Force Statement Before the House Committee on Science, Space, and Technology – Subcommittee on Research and Technology," May 11, 2022

5. (U) "Department of Defense Information Technology, Cybersecurity and Information Assurance for Fiscal Year 2022," Acting CIO for the DoD Statement Before the House Armed Services Committee - Subcommittee on Cyber, Innovative Technologies, and Information Systems, June 29, 2021

6. (U) "Cyber Workforce," Acting CIO for the DoD Statement Before the Senate Armed Services Committee – Subcommittee on Personnel, April 21, 2021

7. (U) "Future Cybersecurity Architectures," Joint DoD Statement Before the Senate Armed Services Committee - Subcommittee on Cybersecurity, April 14, 2021

(U) Appendix C

(U) Reports Identifying Risks by NIST Cybersecurity Framework Category

(~~CUI~~) 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-22-105834			X					X															
GAO-22-104560			X				X																
GAO-22-104765	X								X														
GAO-22-104746																X	X			X			
GAO-22-104679			X						X														
GAO-22-105530			X							X													
GAO-22-104422	X																						
GAO-21-105283										X													
[redacted]	X		X	X	X																		
GAO-21-351			X		X																		
GAO-21-278	X		X		X	X	X							X									
GAO-21-222			X							X				X									
GAO-21-279					X																		
GAO-21-288			X			X			X	X													

~~(CUI)~~

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

(~~CUI~~) 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 (cont'd)																							
GAO-21-256SU	X			X	X																		
GAO-21-179			X				X																
GAO-21-158			X																				
GAO-21-182		X								X													
GAO-21-68			X																				
GAO-20-252	X		X																				
GAO-20-629			X																				
GAO-20-249SP		X		X																			(~~CUI~~)

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

(~~CUI~~) 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-2022-092			X																				
DoDIG-2022-089							X			X													
DoDIG-2022-061				X			X		X	X		X		X									
DoDIG-2022-041					X																		
DoDIG-2021-131					X																		
DoDIG-2021-125						X																	
DoDIG-2021-110	X																						
DoDIG-2021-100			X		X																		
[redacted]							X		X			X											
DoDIG-2021-065				X			X		X														
DoDIG-2021-064							X	X															
DoDIG-2021-050					X																		
DoDIG-2021-051			X				X							X									
DoDIG-2021-043		X																					
DoDIG-2021-001			X				X																(~~CUI~~)

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

(~~CUI~~) 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																							
A-2022-0042-AXZ			X							X													
[redacted]									X														
A-2022-0033-IIZ	X			X	X			X															
A-2022-0026-AXZ									X														
A-2022-0015-AXZ	X					X																	
[redacted]			X																				
[redacted]			X							X									X				
[redacted]			X					X	X	X													
A-2021-0051-AXZ			X																				
[redacted]	X																						
A-2021-0044-AXZ			X											X									
A-2021-0038-AXZ		X	X																				
A-2021-0031-AXZ	X		X			X																	
A-2021-0028-AXZ	X		X																				
[redacted]	X		X	X																			
[redacted]	X						X	X															

(~~CUI~~)

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

(~~CUI~~) 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
Naval Audit Service																							
[redacted]			X																				
[redacted]							X																
[redacted]			X	X					X														
[redacted]						X			X														
[redacted]																	X						
[redacted]																	X	X					
[redacted]	X							X															
[redacted]				X	X																		
[redacted]				X																			
[redacted]				X																			
[redacted]							X																(~~CUI~~)

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

~~(CUI)~~ 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																							
F2022-0012-RWP000	X		X				X		X	X													
F2022-0011-RWC000	X							X															
F2022-0017-REE000	X						X																
F2022-0024-REG000 (Report is CUI)			X							X													
F2022-0008-RES000 (Report is CUI)			X							X													
F2022-0009-O10000							X			X													
F2022-0010-O10000							X			X													
F2022-0013-REE000			X				X		X					X									
F2022-0008-O10000							X					X											
F2022-0007-O10000							X					X		X									
F2022-0012-REG000 (Report is CUI)	X		X					X															
F2022-0006-O10000			X						X														
F2022-0005-O10000							X																
F2022-0004-O10000							X																
F2022-0003-O10000							X					X											
F2022-0002-O10000 (Report is CUI)			X				X																
[redacted]	X		X	X			X			X				X									~~(CUI)~~

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

(~~CUI~~) 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)																							
F2022-0001-RWI000 (Report is CUI)				X						X													
[redacted]	X		X					X	X	X		X											
F2022-0003-REG000	X																						
F2022-0002-REG000	X		X							X													
[redacted]	X			X					X	X													
[redacted]	X		X	X				X		X													
[redacted]	X		X																				
F2021-0007-O10000	X							X						X	X								
[redacted]	X						X		X					X									
[redacted]	X		X	X				X		X				X									
[redacted]	X		X							X													
[redacted]	X						X																
F2021-0010-O30000							X			X				X									
[redacted]	X		X				X			X				X									
F2021-0012-RWC000												X											
F2021-0005-O20000																						X	(~~CUI~~)

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

(~~CUI~~) 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)																							
F2021-0024-RWI000	X						X																
[redacted]												X											
[redacted]	X		X	X				X	X														
F2021-0004-O10000					X			X		X					X				X				
[redacted]			X				X					X											
F2021-0004-O30000							X																
F2021-0002-O10000							X			X		X					X						
[redacted]							X			X				X									
F2021-0006-RWT000									X														
F2021-0007-REA000	X		X		X																		
F2021-0006-RWP000								X			X												
F2021-0008-REG000					X			X		X				X									
F2021-0004-RES000			X					X						X									
F2021-0002-RES000	X		X		X			X						X									
F2021-0001-REN000			X																				
F2020-0043-REO000	X		X																				
F2020-0041-REO000	X									X													(~~CUI~~)

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

(~~CUI~~) 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)																							
F2020-0014-O10000							X			X		X					X						
F2020-0021-RWP000	X																						(~~CUI~~)

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

(~~CUI~~) 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
Other DoD Agencies																							
[redacted]	X		X							X													
AUD-2021-002-U			X	X			X																
[redacted]			X	X																			
[redacted]	X		X												X	X							
21-IG31-007										X													
[redacted]	X		X				X			X													
[redacted]			X					X						X									
[redacted]										X													(~~CUI~~)

-

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

(U)	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	42	4	58	19	15	6	37	19	19	35	1	11	0	18	3	2	5	1	2	1	0	1	0
Classified Reports Subtotal	4	1	6	2	2	1	3	2	1	5	1	2	0	3	0	0	1	0	0	1	0	0	0
Grand Total	**46**	**5**	**64**	**21**	**17**	**7**	**40**	**21**	**20**	**40**	**2**	**13**	**0**	**21**	**3**	**2**	**6**	**1**	**2**	**2**	**0**	**1**	**0** **(U)**

(U) Note: Totals may not equal the number of reports identified because one report may cover more than one NIST Cybersecurity Framework category.

(U) Source: The DoD OIG.

(U) Appendix D

(U) Open Recommendations by NIST Cybersecurity Framework Category

~~(CUI)~~ 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-22-105834			5					2															
GAO-22-104679			3																				
GAO-21-105283										2													
[redacted]	1		4	2	3																		
GAO-21-351			1		1																		
GAO-21-278			2		2		1																
GAO-21-222										1													
GAO-21-256SU					1																		
GAO-21-179			2																				
GAO-21-158			1																				
GAO-20-252	2		3																				
GAO-20-629			1																				

~~(CUI)~~

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

(~~CUI~~) 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-2022-092			7																				
DODIG-2022-089							1			3													
DODIG-2022-061				1			4					1											
DODIG-2022-041					3																		
DODIG-2021-125						3																	
DODIG-2021-110	3																						
DODIG-2021-100					2																		
[redacted]							8																
DODIG-2021-065				1			1																
DODIG-2021-064							2	1															
DODIG-2021-043		4																					(~~CUI~~)

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

(~~CUI~~) 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																							
A-2022-0042-AXZ										3													
[redacted]									4														
A-2022-0033-IIZ	1			1	2			1															
A-2022-0026-AXZ									1														
A-2022-0015-AXZ	2																						
[redacted]			4																				
[redacted]									1														
A-2021-0051-AXZ			1																				
[redacted]	2																						
A-2021-0044-AXZ			1																				
A-2021-0038-AXZ		1	3																				
A-2021-0031-AXZ	2																						
A-2021-0028-AXZ			3																				
[redacted]							1																

(~~CUI~~)

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

(~~CUI~~) 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
Naval Audit Service																							
[redacted]			2	3																			
[redacted]					1																		
[redacted]				3																			
[redacted]			2																				(~~CUI~~)

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

(~~CUI~~) 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																							
F2022-0012-RWP000	2																						
F2022-0011-RWC000	3							1															
F2022-0017-REE000	3						1																
F2022-0024-REG000 (Report is CUI)			1							2													
F2022-0009-O10000							1																
F2022-0013-REE000			2				1		1														
F2022-0012-REG000 (Report is CUI)	1							1															
F2022-0002-O10000 (Report is CUI)			1																				
[redacted]							1																
F2022-0002-REO000 (Report is CUI)	1		2					1	1	4		1											
[redacted]	1			1						1													
F2022-0001-REE000 (Report is CUI)			3							1													
[redacted]			3																				
F2021-0007-O10000	2						1	1		1				2									
[redacted]	2								1					2									
[redacted]	1									1													
[redacted]	1		1							2													

(~~CUI~~)

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

~~(CUI)~~ 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)																							
~~(CUI)~~ [redacted]			1																				
~~(CUI)~~ [redacted]												4											
~~(CUI)~~ [redacted]			1																				
F2021-0002-RES000								1															
F2021-0001-REN000			1																				
F2020-0041-REO000			2																				~~(CUI)~~

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

(~~CUI~~) 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
Other DoD Agencies																							
[redacted]										2													
[redacted]			1																				
[redacted]			8																				
21_IG31_007										1													(~~CUI~~)

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

(U)	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	30	5	72	12	15	3	23	9	9	24	0	6	0	4	0	0	0	0	0	0	0	0	0
Classified Reports Subtotal	4	0	12	7	0	6	8	3	1	5	1	3	0	3	0	0	0	0	0	1	0	0	0
Grand Total	**34**	**5**	**84**	**19**	**15**	**9**	**31**	**12**	**10**	**29**	**1**	**9**	**0**	**7**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**0** **(U)**

(U) Note: Totals may not equal the number of reports identified because one report may cover more than one NIST Cybersecurity Framework category.

(U) Source: The DoD OIG.

(U) Acronyms and Abbreviations

(U) AAA	Army Audit Agency
(U) AFAA	Air Force Audit Agency
(U) CIO	Chief Information Officer
(U) CUI	Controlled Unclassified Information
(U) DISA	Defense Information Systems Agency
(U) GAO	Government Accountability Office
(U) IT	Information Technology
(U) NAVAUDSVC	Naval Audit Service
(U) NFR	Notice of Findings and Recommendations
(U) NIST	National Institute of Standards and Technology
(U) OIG	Office of Inspector General
(U) RMF	Risk Management Framework

INSPECTOR GENERAL

INTEGRITY EFFICIENCY

DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, 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