Report No. DODIG-2019-044

~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

JANUARY 9, 2019

Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

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

~~FOR OFFICIAL USE ONLY~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018

January 9, 2019

Objective

Our objective was to (1) summarize unclassified and classified reports issued and testimonies made from the DoD oversight community and the Government Accountability Office (GAO) between July 1, 2017, and June 30, 2018, that included DoD cybersecurity issues; (2) identify cybersecurity risk areas for DoD management to address based on the five functions of the National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018 (Cybersecurity Framework); and (3) identify the open DoD cybersecurity recommendations.[1]

This summary report also addresses the Federal Information Security Modernization Act of 2014 (FISMA) requirement to provide an annual independent evaluation of the agency's information security program by using the identified findings to support the responses made in our assessment.[2]

Background

On February 12, 2013, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." Executive Order 13636 calls for the development of a voluntary cybersecurity framework for Federal and non-Federal entities that provides a prioritized, flexible, repeatable, performance-based, and cost effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The resulting NIST Cybersecurity Framework was established through collaboration between the Government and private sector entities. The framework has five functions, representing high-level cybersecurity activities that provide a strategic view of the risk management lifecycle—Identify, Protect, Detect, Respond, and Recover. On May 11, 2017, the President mandated that Federal agencies use the NIST Cybersecurity Framework to manage their cybersecurity risks by issuing Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."

FISMA requires that each Federal agency conduct an annual independent evaluation to determine the effectiveness of the agency's information security program and practices. For an agency with an Inspector General (IG) appointed under the IG Act of 1978, that IG, or an independent external auditor designated by that IG, must conduct the annual independent evaluation and report the results to the agency Chief Information Officer by October 31st of each year. The evaluation may be based in whole or in part on an audit, evaluation, or report relating to agency programs or practices. The IG must report the results of the annual independent evaluation to the Office of Management and Budget.

We used this summary report to develop the annual DoD OIG independent evaluation and to meet the reporting requirement, which we communicated to the DoD Chief Information Officer on October 31, 2018.

[1] Open recommendations can be either resolved or unresolved. Resolved recommendations are those that DoD management has agreed to implement but has not yet completed agreed-upon actions. Unresolved recommendations are those that DoD management disagrees with or provide alternative corrective actions.

[2] Public Law 106 531, "Reports Consolidation Act of 2000," Section 3516(d), November 22, 2000, and Public Law 113-283, "Federal Information Security Modernization Act of 2014," Section 3555, December 18, 2014.

Results in Brief

Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018

Summary

We found that DoD Components implemented many of the agreed-upon corrective actions necessary to improve system weaknesses identified in issued reports summarized in our FY 2017 cybersecurity summary report; however, recently issued cybersecurity reports indicate that the DoD still faces challenges in managing cybersecurity risk to its network. Additionally, as of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008.

This year's summary includes the results of 20 unclassified and 4 classified reports issued by the DoD oversight community and GAO between July 1, 2017, and June 30, 2018, relating to DoD cybersecurity. We did not identify any testimonies made by the DoD oversight community and GAO relating to DoD cybersecurity during this period.

The unclassified reports identified improvements in the asset management, information protection processes and procedures, identity management and access control, and security continuous monitoring. We also determined that the DoD has taken action to strengthen its cybersecurity posture by implementing actions to address 19 of the 159 recommendations made in those reports.

~~(FOUO)~~ However, the DoD needs to continue focusing on managing cybersecurity risks related to governance, asset management, information protection processes and procedures, identity management and access control, security continuous monitoring, detection processes, and communications. The largest number of weaknesses identified in this year's summary were related to governance, which allows an organization to inform its management of cybersecurity risk through the policies, procedures, and processes to manage and monitor the organizations regulatory, legal, risk, environmental, and operational requirements. [redacted]

Without proper governance, the DoD cannot ensure that it effectively identifies and manages cybersecurity risk as it continues to face a growing variety of cyber threats from adversaries, such as offensive cyberspace operations used to disrupt, degrade, or destroy targeted information systems. The DoD must also ensure that cybersecurity risks are effectively managed to safeguard its reliance on cyberspace to support its operations and implement proper controls and processes where weaknesses are identified to improve the overall cybersecurity.

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

January 9, 2019

MEMORANDUM FOR DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER
COMMANDER, U.S. CYBER COMMAND
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE
MANAGING DIRECTOR, INFORMATION TECHNOLOGY, GOVERNMENT ACCOUNTABILITY OFFICE

SUBJECT: Summary of Reports Issued Regarding Department of Defense Cybersecurity From July 1, 2017, Through June 30, 2018 (Report No. DODIG-2019-044)

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

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

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

Contents

Introduction

Objective

Our objective was to (1) summarize unclassified and classified cybersecurity reports issued and testimonies given by the DoD oversight community and the Government Accountability Office (GAO) issued between July 1, 2017, and June 30, 2018; (2) identify cybersecurity risk areas for DoD management to address based on the five functions of the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity," April 16, 2018 (Cybersecurity Framework); and (3) identify the open DoD cybersecurity recommendations.[3] This summary will also address the Federal Information Security Modernization Act of 2014 (FISMA) requirement to provide an annual independent evaluation of the agency's information security program by using the identified findings to support the responses made in our assessment.[4]

See Appendix A for a discussion on the scope and methodology and a list of previously issued cybersecurity summary reports. See Appendix B for a list of the unclassified and classified reports summarized in this report. See Appendix C for risks identified by Inspector General (IG) FISMA Reporting Metric. See Appendixes G and H for summaries of the identified classified cybersecurity reports.

Background

The DoD depends on cyberspace to support its operations and, therefore, must be able to secure its networks against attack or recover quickly if security measures fail. Cybersecurity risk management comprises the full range of activities undertaken to protect information and information technology from cyber threats such as unauthorized access and loss of data. DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, establishes the DoD Cybersecurity Program to protect and defend DoD information and information technology. According to the Instruction, all DoD information technology must be assigned to, and governed by, a DoD Component cybersecurity program that manages risk commensurate with the importance of supported missions and the value of potentially affected information and assets. This summary report provides a reference for identifying reports

[3] Open recommendations can be either resolved or unresolved. Resolved recommendations are those that DoD management has agreed to implement, but has not yet completed agreed-upon actions. Unresolved recommendations are those that DoD management disagrees with or provides alternative corrective actions for.

[4] Public Law 106-531, "Reports Consolidation Act of 2000," Section 3516(d), November 22, 2000, and Public Law 113-283, "Federal Information Security Modernization Act of 2014," Section 3555, December 18, 2014.

outlining DoD cybersecurity risks using the NIST Cybersecurity Framework and the "FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics," May 24, 2018 (IG FISMA Reporting Metrics).

NIST Cybersecurity Framework

Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," February 12, 2013, required NIST to develop a voluntary cybersecurity framework that provides a prioritized, flexible, repeatable, performance-based, and cost effective approach to help the owners and operators of critical infrastructure identify, assess, and manage cyber risk. The Cybersecurity Enhancement Act of 2014 further codified requirements for NIST to develop an approach to help identify, assess, and manage cyber risk for critical infrastructure.

In May 2017, the President mandated that Federal agencies use the NIST Cybersecurity Framework to manage their cybersecurity risk. Specifically, Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," May 11, 2017, states that the President will hold heads of executive departments and agencies accountable for managing cybersecurity risk to their enterprises. Furthermore, the executive order requires that each agency head use the NIST Cybersecurity Framework, or any successor document, to manage the agency's cybersecurity risk.

The NIST Cybersecurity Framework establishes a risk-based approach to managing cybersecurity risk by providing an organization with a common set of cybersecurity activities, desired outcomes, and criteria.[5] This allows the organization to communicate using a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. The Framework can be used to help identify and prioritize actions for reducing cybersecurity risk and is a tool for aligning policy, business, and technological approaches to managing that risk.

Framework Functions

The Framework core has five functions—Identify, Protect, Detect, Respond, and Recover—representing high-level cybersecurity activities that provide a strategic view of the risk management lifecycle. Table 1 lists the five functions and the corresponding high-level, cybersecurity activities.

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

Table 1. NIST Cybersecurity Framework

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

Source: NIST Cybersecurity Framework.

Framework Categories

The 5 NIST functions include 23 associated categories that provide desired cybersecurity outcomes. Each of the 23 categories also has anywhere from 4 to 12 subcategories that enable an organization to manage its cybersecurity risk when the actions are performed. See Table 2 for the Framework's 23 categories and the desired cybersecurity outcomes of each category by function.

Table 2. NIST Cybersecurity Framework Categories

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

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

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

Source: NIST Cybersecurity Framework.

Risk Management and the Cybersecurity Framework

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

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

Summary

Managing Cybersecurity Risks Remains a Challenge for DoD Despite Improvements Made in Some Framework Categories

We found that DoD Components implemented many of the agreed-upon corrective actions necessary to improve system weaknesses identified in the reports summarized in our FY 2017 cybersecurity summary report; however, recently issued cybersecurity reports indicate that the DoD still faces challenges in managing cybersecurity risk to its network. Additionally, as of September 30, 2018, there were 266 open cybersecurity-related recommendations, dating as far back as 2008.

This year's summary includes the results of 20 unclassified and 4 classified reports issued by the DoD oversight community and GAO between July 1, 2017, and June 30, 2018, relating to DoD cybersecurity.[6] We did not identify any testimonies made by the DoD oversight community and GAO relating to DoD cybersecurity during this period. The 20 unclassified reports indicate that the DoD made improvements in the Framework categories of asset management, information protection processes and procedures, identity management and access control, and security continuous monitoring.[7] We also determined that the DoD has taken actions to strengthen its cybersecurity posture by implementing actions to address 19 of the 159 recommendations made in those reports.

~~(FOUO)~~ However, the DoD needs to continue focusing on managing cybersecurity activities in four of the five NIST Cybersecurity Framework functions—Identify, Protect, Detect, and Respond, primarily in the Framework categories of governance, asset management, information protection processes and procedures, identity management and access control, security continuous monitoring, detection processes, and communications. The largest number of weaknesses identified in this year's summary were related to the Governance category (under the Identify function), which allows an organization to inform its management of cybersecurity risk through the policies, procedures, and processes to manage and monitor the organizations regulatory, legal, risk, environmental, and operational requirements.

[redacted]

[6] See Appendixes G and H for information on classified cybersecurity-related reports issued during this time period.

[7] We considered improvements when we identified cybersecurity reports that verified the DoD Components implemented the necessary corrective action to close a recommendation.

Without proper governance, the DoD cannot assure that it effectively identifies and manages cybersecurity risk as it continues to face a growing variety of cyber threats from adversaries such as offensive cyberspace operations used to disrupt, degrade, or destroy targeted information systems. The DoD must ensure that cybersecurity risks are effectively managed to safeguard its reliance on cyberspace to support its operations and implement proper controls and processes where weaknesses are identified to improve cybersecurity for the DoD. See Appendix D for a matrix of reports organized by NIST Cybersecurity Framework function.[8]

Challenges Remain in Managing Cybersecurity Risk

~~(FOUO)~~ Although we were able to identify examples of strengths and instances where DoD Components implemented the agreed-upon corrective actions necessary to improve identified system weaknesses for some Framework categories since our FY 2017 cybersecurity summary report, recently issued DoD oversight community and GAO reports indicate that the DoD still faces challenges in managing its cybersecurity risk. Specifically, this year's summary identifies that overall, the DoD needs to continue focusing on managing cybersecurity activities in the Framework categories of governance, asset management, information protection processes and procedures, identity management and access control, security continuous monitoring, detection processes, and communications. The largest number of weaknesses identified in this year's summary are in the Governance category, under the Identify function. [redacted] Without proper governance, the DoD cannot ensure that it uses policies, processes, and procedures to effectively identify and manage cybersecurity risk.

~~(FOUO)~~ [redacted]

Without adequate controls in those subcategories, the DoD cannot ensure that all of its systems, devices, personnel, and vulnerabilities are identified and managed; that all DoD information is protected from unauthorized access; or that all DoD Components are prepared to react to a disruption in system availability.

[8] The matrix does not include the Respond function because only one report addressed this area and is summarized in the body of the report, or the Recover function because there were no reports issued that addressed this area.

~~(FOUO)~~ [redacted]

As of September 30, 2018, we identified that the DoD also needs to take action to close 266 open DoD cybersecurity-related recommendations—255 unclassified and 11 classified—made in issued reports, dating as far back as 2008. The open recommendations primarily focus on the Identify and Protect functions. As the DoD continues to face a growing variety of cyber threats from adversaries, such as offensive cyberspace operations used to disrupt, degrade, or destroy targeted information systems, the DoD must ensure that cybersecurity risks are effectively managed to safeguard its reliance on cyberspace to support its operations.

Risks by NIST Cybersecurity Framework

The DoD oversight community and the GAO issued 20 unclassified and 4 classified reports from July 1, 2017, through June 30, 2018 that identified cybersecurity weaknesses in four of the five functions—Identify, Protect, Detect, and Respond. We also identified 151 open recommendations from those reports as of September 30, 2018. See Table 3 for the number of reports we identified that addressed each NIST Cybersecurity Framework function.

Table 3. Reports by NIST Cybersecurity Framework Function

Function	GAO	DoD OIG	Navy	Air Force	Other	Total
Identify	6	6	2	7	2	**23**
Protect	4	5	2	4	2	**17**
Detect	-	3	-	2	1	**6**
Respond	-	-	1	-	-	**1**
Recover	-	-	-	-	-	**-**

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

Source: The DoD OIG.

[redacted]

Identify Function

We identified 19 unclassified and 4 classified reports addressing the Identify function, primarily within the categories of governance and asset management. The Identify function includes those activities that assist an organization with developing an understanding for managing cybersecurity risk to systems, people, assets, data, and capabilities.

~~(FOUO)~~ Additionally, the reports identified risks in three of the four remaining categories under the Identify function—business environment, risk assessment, and supply chain risk management—such as:

- [redacted]
- [redacted]
- [redacted]

To address the cybersecurity risks in the Identify function, DoD needs policies and controls in place for understanding the business context, the resources that support critical functions, and to prioritize its efforts based on its risk management strategy and business needs. The NIST Cybersecurity Framework provides standards and guidelines such as NIST Special Publications and other common practices that can be implemented to achieve the outcomes associated with each subcategory of the Identify function. The following sections provide examples of unclassified reports that identified weaknesses in the two main categories under the Identify function—Governance and Asset Management.

Governance Category

~~(FOUO)~~ We identified 16 unclassified and 3 classified reports addressing the Governance category. The Framework defines Governance category outcomes as those that allow an organization to inform its management of cybersecurity risk through the policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements. [redacted] Table 4 provides a summary of key report findings by Governance subcategory.

(FOUO) Table 4. Key Report Findings Addressing Governance Subcategories

[redacted]						
[redacted]	I	I	I	I	I	I
[redacted]	I	I	I	I	I	I
[redacted]	I	I	I	I	I	I

Legend

I Improvement
W Weakness
- No Improvements or Weaknesses Identified

Source: The DoD OIG.

(FOUO) The reports identified an improvement in the Governance category relating to cybersecurity guidance. Specifically, the DoD updated its cybersecurity policy to include requirements for officials performing vulnerability assessments as well as preparing and approving formal risk assessments before outsourcing key cybersecurity services. [redacted] The following unclassified reports provide an example of how governance affects DoD operations.

DCMA Report No. DCMA-DMI-2017-001, "Audit of Cybersecurity Workforce Management," July 26, 2017

The DCMA Office of Internal Audit and Inspector General found that DCMA had established policies and procedures in place to manage its cyber workforce. However, there were gaps relating to cyber workforce identification, classification, and training. Specifically, there was not an effective process to identify cyber positions across all DCMA directorates and sub-directorates; train the cyber workforce to meet certification requirements; address employee non-compliance with certification requirements; and participate in DoD Chief Information Officer (CIO) working group for cyber workforce improvement. The DCMA Cybersecurity Center managed DCMA's "8570" program using a SharePoint library, referred to as the 8570 tracker, to track known cyber personnel.[10] The DCMA Office of Internal Audit and Inspector General tested the completeness and accuracy of the 8570 tracker and found that the DCMA Cybersecurity Center

[10] DoD Directive 8140.01 "Cyberspace Workforce Management" updated and expanded established policies and assigned responsibilities for managing the DoD cyberspace workforce, formerly found in DoD Directive 8570.01.

only had visibility over 212 of 496 (42.7 percent) of the IT Specialists identified using the authoritative civilian manpower data from the DoD Fourth Estate Manpower Tracking System. The lack of visibility over manpower data occurred because there was no process in place to compare records in the 8570 tracker to existing manpower data. Additionally, position descriptions may not have had the 8570 requirement. This lack of visibility created issues with ensuring cyber workers received proper resources and training to obtain required certifications.

The DCMA Office of Internal Audit and Inspector General also found that 48 of the 176 (27.3 percent) records marked compliant did not have supporting documentation showing the employee obtained required certifications. These inaccuracies occurred due to two internal control weaknesses. First, employees could indicate whether they were compliant or the requirement did not apply without any further review or approval by a supervisor or other third party. Second, DCMA Cybersecurity Center personnel responsible for the tracking database did not have an effective monitoring system to ensure each record was accurate. As a result, DCMA lacked complete visibility of its cyber workforce and whether they were certified in accordance with DoD requirements. This caused the IT Scorecard submitted to DoD to include inaccurate 8570 compliance information.

DCMA Office of Independent Assessment recommended that that the DCMA CIO require a higher level review for employees who were self-certifying their compliance in the 8570 tracker. They also recommended that the CIO and the Director, Human Capital:

- establish a process to identify the full universe of the DCMA Cyber Workforce in existing personnel databases, including establishing 8570 compliance requirements for all impacted civilian positions as well as including the requirements for all applicable contracted services; and
- determine the appropriate actions to take for employees that failed to meet 8570 requirements.

The DCMA CIO and the Director, Human Capital concurred with all of these recommendations and their comments were considered responsive. As of September 30, 2018, the recommendations remained open.

GAO Report No. GAO-18-211, "Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption," February 15, 2018

The GAO found that the DoD did not take steps to facilitate use of the NIST Cybersecurity Framework and had not taken actions to measure the implementation of the framework within the Defense Industrial Base. Specifically, GAO stated that the DoD did not develop implementation guidance that addresses

how the Defense Industrial Base can adopt the framework.[11] Presidential Policy Directive 21 establishes the DoD as the Federal entity responsible for leading, facilitating, or supporting resilience programs and associated activities for the Defense Industrial Base, which is designated as one of the nation's 16 critical infrastructure sectors.[12] In addition, Executive Order 13636 directed the DoD, in consultation with the Department of Homeland Security and other interested agencies, to review the cybersecurity framework and, if necessary, develop implementation guidance or supplemental materials to address risks and operating environments for individual infrastructure sectors. However, the DoD did not develop an implementation guide and did not know the extent to which the framework had been adopted within the Defense Industrial Base. DoD officials stated that Defense Industrial Base officials, while interested in the framework, generally had not fully implemented it because their agencies follow cybersecurity-related requirements established in the Defense Federal Acquisition Supplement, "Safeguarding Covered Defense Information and Cyber Incident Reporting." Officials from the eight agencies associated with the critical infrastructure sectors reported the following challenges in adopting the framework.[13]

- Entities may be limited in their ability to commit necessary resources toward framework adoption.
- Entities may not have the necessary knowledge and skills to effectively implement the framework.
- Entities may face regulatory, industry, and other requirements that inhibit adopting the framework.
- Entities may face other priorities that take precedence over conducting cyber-related risk management or adopting the framework.

The DoD officials under review stated that they did not have a mechanism to assess overall use of the framework because its use by the Defense Industrial Base is voluntary. However, the GAO stated that until the DoD has a more comprehensive understanding of the use of the cybersecurity framework by entities within its critical infrastructure sector, the DoD will be limited in its ability to understand the success of protection efforts or to determine where to focus its limited resources for cyber risk mitigation.

---

[11] The Defense Industrial Base is a critical infrastructure sector that supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology, supply, and maintenance.

[12] The 16 critical infrastructure sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

[13] Sector-specific agencies include the Departments of Defense, Agriculture, Energy, Health and Human Services, Homeland Security, Treasury, Transportation, the Environmental Protection Agency, and the General Services Administration. Entities include sector-specific agencies and the sector coordinating councils.

GAO recommended that the Secretary of Defense take steps to consult with its respective sector partner(s), such as the sector coordinating councils, the Department of Homeland Security, and NIST, as appropriate, to develop a process for determining the level and type of framework adoption by entities across their respective sectors.[14] The Acting Deputy CIO for Cybersecurity concurred with the recommendation. As of September 30, 2018, the recommendation remained open.

Governance Category Takeaways

As discussed in the examples above, these 19 reports identified risks in the Governance category. The report identified issues relating to cyber workforce identification, classification of positions that should be part of the cyber workforce, training to meet certification requirements, and guidance to address risks and operating environments. As a result, the DoD should ensure that policies are established and communicated and that governance and risk management processes address the appropriate cybersecurity risks.

Asset Management Category

~~(FOUO)~~ We identified 10 unclassified and 2 classified reports addressing the Asset Management category. The Framework defines the Asset Management category outcomes as those actions that allow an organization to identify and manage its resources, such as systems, devices, and personnel, to achieve business purposes. [redacted] For improvements, DoD OIG verified that the Defense Manpower Data Center's Configuration Management Database server and related equipment entries were now accurate and complete.[15] [redacted] Table 5 provides a summary of key report findings by Asset Management subcategory.

[14] Sector coordinating councils were formed to serve as the voice of each sector and principal entry point for the Government to collaborate with each sector. Sector coordinating councils are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities.

[15] DoD OIG verified the improvements during a follow-up audit.

(FOUO) Table 5. Key Report Findings Addressing Asset Management Subcategories

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	I	I	I	I	I	I
[redacted]	I	I	I	I	I	I

Legend

I Improvement
W Weakness
- No Improvements or Weaknesses Identified

Source: The DoD OIG.

(FOUO) The reports identified improvements in the Asset Management category such as maintaining accurate and complete records for devices and defining information assurance roles and responsibilities. [redacted]

The following unclassified Air Force Audit Agency (AFAA) reports describe how asset management affects DoD operations.

AFAA Report No. F2018-0001-O10000, "Wireless Network," October 10, 2017

The AFAA found that Air Force personnel did not account for and physically secure wireless network access points in accordance with Air Force guidance.[16] In addition, AFAA found that at all 15 installations reviewed, personnel did not account for 8,852 of 8,951 (99 percent) wireless devices in the Air Force Equipment Management System–Asset Inventory Management as required by Air Force Manual 33-153. AFAA also found that personnel at 8 of the 15 installations could not locate 274 of 1,019 (26.9 percent) statistically selected devices. This occurred because Communications Squadron personnel did not comply with existing guidance to account for sensitive assets in the equipment management system. Furthermore, 38th Cyberspace Readiness Squadron personnel did not establish an internal control process to ensure that Communications Squadron personnel properly accounted for wireless assets.[17] Properly accounting for and securing wireless network assets reduces the risk of fraud, waste, and theft. By not accounting for wireless assets in the Asset Inventory Management system, Air Force financial statements were understated by at least $52.5 million, which undermines the Air Force's ability to comply with Financial Improvement and Audit Readiness requirements and achieve auditable financial statements by the end of 2017.

[16] A wireless access point allows devices to connect to a wired network using wi-fi, or related standards.

[17] The 38th Cyberspace Readiness Squadron serves as the Air Force Equipment Control Office for all Air Force information technology hardware.

The AFAA recommended that the Commander for the Air Force Space Command Integrated Air, Space, Cyberspace, and Intelligence, Surveillance, and Reconnaissance Operation direct 38th Cyberspace Readiness Squadron personnel to issue guidance requiring Air Force Communications Squadron personnel to comply with existing information technology asset management guidance for wireless access points in the Air Force Equipment Management System–Asset Inventory Management. The Executive Director for Air Force Space Command responded that, during the audit, Air Force Space Command and 38th Cyberspace Readiness Squadron personnel completed the actions for the recommendation. The AFAA also recommended that the Commander for Air Force Space Command Integrated Air, Space, Cyberspace, and Intelligence, Surveillance, and Reconnaissance Operation direct 38th Cyberspace Readiness Squadron personnel to implement internal control procedures within the Air Force Inspection System which ensure that Communications Squadron personnel comply with Air Force guidance on accounting for and physically securing wireless assets. The Executive Director for Air Force Space Command agreed with the recommendation. As of September 30, 2018, the two recommendations to the Air Force Space Command are closed.

AFAA Report No. F2018-0002-O10000, "Air Force Information Network (AFIN) and Air Force Network (AFNET) Data Call Validation," November 8, 2017

The AFAA found that Air Force personnel did not accurately identify the universe of information technology that comprises the Air Force Information Network. The Air Force Office of the Chief, Information Dominance and CIO created a Task Management Tool tasker requiring Major Commands, National Guard, and Reserve personnel to identify information technology. However, personnel did not distribute the tasker to direct reporting units. They also allowed the units to determine their own methodology for compiling the list of information technology, and did not receive responses from all units tasked or follow up with those units. This resulted in a total of only 285 information technology systems being reported in the Task Management Tool. Recent system audits at limited locations found almost 2,400 information technology systems not previously identified in the Tool. This occurred because the Air Force Office of the Chief, Information Dominance and CIO did not develop effective procedures to identify the universe of information technology that comprises the Air Force Information Network. In addition, there was not a standard, repeatable process to sustain complete system information in the Air Force repository. Finally, there was no mechanism in place to enforce system registration if not connected to the AFNET. Accurately identifying the universe of information technology that comprises the Air Force Information Network would lead to an effective cybersecurity posture and the ability to achieve mission assurance across the enterprise.

The AFAA made several recommendations, including that the Air Force Chief, Information Dominance and CIO direct the Chief Information Security Officer to develop effective procedures to identify the universe of information technology that comprises the Air Force Information Network. The Air Force Chief, Information Dominance and CIO responded that his office would coordinate with Air Force Space Command, Authorizing Officials, Acquisition Community, and Portfolio Managers to ensure that all information technology comprising the Air Force Information Network are identified. In addition, the office would provide oversight for Air Force guidance requiring information technology to be registered in the official repository, the Information Technology Investment Portfolio System. The AFAA considered the management comments and planned actions responsive and addressed the recommendations. As of September 30, 2018, however, the three recommendations to the Air Force Space Command remained open.

Asset Management Category Takeaways

As discussed in the examples above, these 12 reports identified cybersecurity risks within the Asset Management Category by identifying organizations that did not account and physically secure wireless access points nor accurately identify the universe of information technology that comprised their network. As a result, the organizations should ensure that physical devices and systems within their organization are inventoried to mitigate the cybersecurity risks within their organization.

Protect Function

We identified 16 unclassified reports and 1 classified report addressing the Protect function, primarily within the Information Protection Processes and Procedures and the Identity Management and Access Controls categories. The Protect function includes those activities that assist the organization to develop and implement appropriate safeguards to ensure delivery of critical services.

~~(FOUO)~~ Additionally, the reports identified improvements and risks in the other four areas of the Protect function—awareness and training, data security, maintenance, and protective technology. These reports identified improvements such as newly developed and updated data sharing agreements for transferring data between organizations. However, these reports also identified weaknesses such as:

- [redacted]
- [redacted]
- [redacted]

To address cybersecurity risk in the Protect function DoD must implement controls, such as monitoring user activity on the network, that support the ability to limit or contain the impact of a potential cybersecurity event. The NIST Cybersecurity Framework provides standards and guidelines such as NIST Special Publications and other common practices that can be implemented to provide achieve the outcomes associated with each subcategory of the Protect function.

The following sections provide examples of unclassified reports that identified weaknesses in the two main categories identified under the Protect function during this reporting period—Information Protection Processes and Procedures and Identity Management and Access Control.

Information Protection Processes and Procedures Category

~~(FOUO)~~ We identified 10 unclassified and 1 classified report addressing the Information Protection Processes and Procedures category. The Framework defines Information Protection Processes and Procedures category outcomes as those that allow an organization to maintain and use security policies, processes, and procedures to manage protection of its information systems and assets. [redacted] For the strengths, DoD submitted Presidential Policy Directive–41 and the Department of Homeland Security's National Cyber incident Response Plan to satisfy one of the elements of the National Defense Authorization Act. Those documents described the roles, responsibilities, and expectations of federal, state, and local authorities to support domestic cyber incident response efforts. [redacted] Table 6 provides a summary of key report findings by Information Protection Processes and Procedures subcategory.

~~(FOUO)~~ *Table 6. Key Report Findings Addressing Information Protection Processes and Procedures Subcategories*

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	I	I	I	I	I
[redacted]	[redacted]	I	I	I	I	I
[redacted]	[redacted]	I	[redacted]	[redacted]	I	I
[redacted]	[redacted]	I	I	I	I	I
[redacted]	I	I	I	I	I	I
[redacted]	I	I	I	[redacted]	I	I
[redacted]	I	[redacted]	[redacted]	[redacted]	I	[redacted]

Legend

I Improvement
S Strength
W Weakness
- No Improvements, Strengths, or Weaknesses Identified

Source: The DoD OIG.

~~(FOUO)~~ The reports identified improvements in the Information Protection Processes and Procedures category where the DMDC updated cybersecurity policy to require officials to implement policies and procedures for managing, configuring, and securing the DMDC network devices. [redacted] The following reports describe how information protection processes and procedures affect DoD operations.

GAO Report No. GAO-18-324, "The Warfighter and Decision Makers Would Benefit from Better Communication about the System's Capabilities and Limitations," May 30, 2018

GAO found that, in fiscal year 2017, the MDA continued to deliver assets to military services, however, system-level integrated capabilities, such as some discrimination and integrated cyber defense improvements, were delayed and delivered with performance limitations. Specifically MDA significantly reduced the content of its Ballistic Missile Defense System (BMDS) cyber defense capability

planned for Increment 4. MDA documentation originally planned to deliver this capability with 10 elements and, prior to testing, the BMDS Operational Test Agency declared four elements to be priorities.[18] Of these four, MDA has conducted the assessment for only three. In recent years, MDA has declared major capabilities ready for delivery through a process that culminates in the issuance of a Technical Capability Declaration (TCD). According to MDA officials, the primary purpose of a TCD is to allow MDA's senior management to manage the delivery of integrated, BMDS-level capabilities that require more than one element to function; however, GAO has found that MDA's process for managing the delivery of BMDS-level capabilities is not applied consistently and has unclear requirements. Specifically, GAO found inconsistencies in MDA's decisions regarding which integrated, BMDS-level capabilities MDA would deliver through a TCD, and which it would not. For example, since 2015, the agency planned to deliver 14 integrated, BMDS-level capabilities, but delivered only 7 through the TCD process. MDA issued a memorandum on Technical Capability Declaration Planning and Definitions in June 2017 to help distinguish element-level Operational Capacity Baseline deliveries and deliveries of integrated BMDS capabilities that would occur via TCD.[19] However, the new policy does not address several important problems with the TCD process. Specifically, it does not identify any criteria or reasoning that guided or will guide MDA to determine to use TCD to deliver capabilities. Unless MDA requires that all integrated capabilities are delivered via the TCD process, as the BMDS becomes more integrated, military services and other decision makers will have reduced insight into the capabilities and limitations of the BMDS as a whole.

GAO recommended that the Director, MDA should revise MDA policies to require that all integrated capabilities—capabilities that require integration of two or more elements—be included in a Technical Capability Declaration. DoD partially concurred with the recommendation and agreed to its intent. Additionally, DoD stated that the Director, MDA would determine which major integrated capabilities should be delivered via the TCD process and noted that the agency developed a list of such capabilities that it will update annually; however, GAO replied that, while these actions were an improvement over the current process, they do not meet the full intent of the recommendation. Specifically, the list of future TCDs that MDA produced is not inclusive of all future integrated capabilities. In addition, MDA's policy does not articulate definitive standards for identifying capabilities requiring a TCD and leaves this decision to the discretion of the Director, MDA. Therefore, GAO continues to believe that in order for the agency to meet the full intent of

[18] MDA is responsible for developing a number of systems, known as elements, with the purpose of defending against ballistic missile attacks.

[19] Typically, MDA makes capability deliveries through approved changes to its Operational Capacity Baseline.

this recommendation, it should establish in policy a clear, definitive standard for which capabilities require a TCD for delivery. As of September 30, 2018 the recommendation remained open.

AFAA Report No. F2018-0003-O10000, "Cybersecurity Program Management Configuration," December 22, 2017

The AFAA found that Assistant Secretary of the Air Force for Acquisition officials, in coordination with the Air Force Chief, Information Dominance, and CIO, did not ensure that cybersecurity was integrated into weapon systems during design. Instead, weapon systems' cybersecurity was addressed through a set of activities and products that were not fully integrated, creating overlaps and gaps in the program cybersecurity.[20] This occurred because the Assistant Secretary of the Air Force for Acquisition, in coordination with the Air Force CIO, did not develop an integrated implementation plan that synchronized functions and organizations tasked with ensuring weapon systems cybersecurity across the Air Force. Cyber capabilities enable many of the advanced features that give the Air Force its edge over potential adversaries. Likewise, adequate cybersecurity direction and planning decreases the risk of failure for the Air Force's weapon systems from unmitigated cyber vulnerabilities.

The AFAA made multiple recommendations, including that the Assistant Secretary of the Air Force for Acquisition, in coordination with the Air Force CIO, initiate action to develop an integrated implementation plan synchronized across the Air Force functions and organizations tasked with ensuring weapon systems cybersecurity. During audit, the Cyber Resiliency Office developed the Fiscal Year 2017 Line of Action Product Dashboard listing the seven lines of action, its respective action plan, and status. The Cyber Resiliency Office's primary focus is to integrate activities across the Air Force to ensure weapon systems maintain mission-effective capabilities, despite cyber adversaries. The AFAA considered management comments and planned actions to be responsive but as of September 30, 2018 the recommendations remained open.

Information Protection Processes and Procedures Category Takeaways

As discussed in the examples above, these 11 reports identified weaknesses in the Information Protection Processes and Procedures Category such as cybersecurity not being integrated into DoD weapon systems design as well as the Services experiencing performance limitations or delays in receiving required assets to complete their missions. As a result, the DoD should ensure that they incorporate all integrated capabilities into the appropriate technical documents for systems and that they integrate cybersecurity into weapon systems during design.

[20] AFAA identified the set of activities and products that were not fully integrated as derived requirements, software assurance, supply chain management, cybersecurity strategy, and program protection plan.

Identity Management and Access Control Category

~~(FOUO)~~ We identified seven unclassified and one classified report addressing Identity Management and Access Control. The Framework defines the Identity Management and Access Control category outcomes as those that allow an organization to limit access to physical and logical assets to authorized users, processes, and devices. [redacted] For the improvements the DMDC enhanced the physical security controls at its data center by installing steel mesh on the windows and glass breakage monitors to protect against unauthorized entry. [redacted] Table 7 provides a summary of key report findings by Identity Management and Access Control subcategory.

~~(FOUO)~~ Table 7. Key Report Findings Addressing Identity Management and Access Control Subcategories

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Legend

I Improvement
W Weakness
- No Improvements or Weaknesses Identified

Source: The DoD OIG.

~~(FOUO)~~ The reports identified improvements such as DMDC updating cybersecurity policy to require officials to establish procedures for granting access, including remote access, to DMDC systems and resources. [redacted] The following unclassified reports describe how identity management, authentication, and access control affects DoD operations.

DoD OIG Report No. DODIG-2017-085, "Protection of Electronic Patient Health Information at Army Military Treatment Facilities," July 6, 2017

The DoD OIG found that the Defense Health Agency (DHA) and Army officials did not always implement security protocols to protect systems that stored, processed, and transmitted electronic health record (EHR) and patient health information. Specifically, DHA and Army officials did not:

- enforce the use of Common Access Cards (CACs) to access the three DoD EHR systems and two Army-specific systems because system administrators stated that the CAC software was incompatible with older system software or did not allow multiple users to log in and out of the systems without rebooting local terminals; and
- comply with DoD password complexity requirements for the Clinical Information System/Essentris Inpatient System (Essentris) and two Army-specific systems because system administrators considered existing network authentication requirements sufficient to control access.

In addition, system and network administrators at the Brooke Army Medical Center, Evans Army Community Hospital, and Kimbrough Ambulatory Care Center did not:

- grant user access to the three DoD EHR systems and four Army-specific systems based on the user's assigned duties because they did not require user justifications for access or align user responsibilities to specific system roles;
- configure two DoD EHR systems and five Army-specific systems to automatically lock after 15 minutes of inactivity because the military treatment facility CIOs did not want to negatively affect system availability; and
- develop standard operating procedures to manage system access because they did not consider documented procedures necessary.

Without well-defined, effectively implemented system security protocols, the DHA and Army introduced unnecessary risks that could compromise the integrity, confidentiality, and availability of patient health information. Security protocols, when not applied or ineffective, increase the risk of cyber-attacks, system and data breaches, data loss or manipulation, and unauthorized disclosures of patient health information. In addition, ineffective administrative, technical, and physical security protocols that result in a Health Insurance Portability and Accountability Act of 1996 violation could cost military treatment facilities up to $1.5 million per year in penalties for each category of violation.

The DoD OIG made 39 recommendations related to the NIST Cybersecurity Framework, including that the CIOs for the DHA, U.S. Army Medical Command, and military treatment facilities implement configuration changes to enforce the

use of CACs when accessing DoD EHR systems and Army-specific systems and configure passwords for the DoD EHR systems and Army-specific systems to meet DoD complexity requirements.[21] The DoD OIG closed three recommendations after the DHA Chief of Staff provided two existing position descriptions and officer evaluation reports for the three Army locations visited that included one or more specific security-related performance standards for complying with security requirements and protecting patient health information. One included standards to hold CIOs accountable for protecting patient health information. Additionally, the DoD OIG considered six recommendations unresolved because the management response to those recommendations and their planned actions did not fully address the identified issues. The DoD OIG considered the remaining 30 recommendations resolved. As of September 30, 2018, 36 of the 39 recommendations remained open.

[redacted][22]

~~(FOUO)~~ [redacted]

[21] The DoD OIG report stated that the U.S. Army Medical Command provides sustained health services for about 4 million active duty members across the Military Services.

[22] [redacted]

(FOUO) [redacted]

Identity Management and Access Control Category Takeaways

(FOUO) The DoD OIG and NAVAUDSVC identified weaknesses in the Identify Management and Access Control Category such as security protocols that were not always implemented to protect systems that stored, processed, and transmitted electronic health records and patient health information and [redacted] As a result, the DoD needs to ensure that identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes.

Detect Function

We identified five unclassified and one classified report addressing the Detect function, primarily within the Security Continuous Monitoring category. The Detect function includes those activities that assist the organization to develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

Additionally, the reports identified strengths or weaknesses in the two of the three categories—security continuous monitoring and detection processes—such as:

- contractors that did not scan workstations to identify vulnerabilities,
- personnel that did not perform periodic security assessments nor monitor wireless network security, and
- personnel that did not have proper approval to operate and monitor social media sites to prevent operational security violations.

However, we did not identify any reports that addressed the Anomalies and Events category, which include detection and analysis of an event that occurs at an agency as well as the impact the event had on the agency. To address cybersecurity risk in the Detect function, the DoD need to implement controls that enable timely discovery of cybersecurity events. The NIST Cybersecurity Framework provides standards and guidelines such as NIST Special Publications and other common practices that can be implemented to achieve the outcomes associated with each subcategory of the Detect function.

The following sections provide examples of unclassified reports that identified weaknesses in the two main categories identified under the Detect function—Security Continuous Monitoring and Detection Processes.

Security Continuous Monitoring Category

~~(FOUO)~~ We identified five unclassified and one classified report addressing Security Continuous Monitoring. The Framework defines Security Continuous Monitoring category outcomes as those that allow an organization to monitor its information systems and assets to identify cybersecurity events and verify effectiveness of protective measures. For example, the reports identified strengths in the Continuous Monitoring subcategory as well as [redacted] For the strengths, Space and Naval Warfare Systems Command were effectively meeting cyber resiliency requirements derived from the National Defense Authorization Act, DoD and Secretary of the Navy instructions, and the cybersecurity safety updated guidance message released on May 2, 2017. Table 8 provides a summary of key report findings by Security Continuous Monitoring subcategory.

~~(FOUO)~~ Table 8. Key Report Findings Addressing Security Continuous Monitoring Subcategories

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Legend

I Improvement
S Strength
W Weakness
- No Improvements, Strengths, or Weaknesses Identified

Source: The DoD OIG.

~~(FOUO)~~ The reports identified strengths and improvements in the Security Continuous Monitoring Category such as one Naval command, ensuring that cyber resiliency requirements were included in contracts, preparing cyber risk assessments, conducting penetration tests, and initiating efforts to enable a continuous monitoring capability. [redacted] The following unclassified reports describe how security continuous monitoring affects DoD operations.

DoD OIG Report No. DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018

The DoD OIG found that three out of seven MDA contractors reviewed did not scan workstations that stored classified ballistic missile defense system technical information to identify vulnerabilities. Specifically, Contractors D and G did not scan workstations that stored classified ballistic missile defense system technical information and only assessed the workstations for compliance with software baselines. The system administrator at Contractor D and the information system security manager at Contractor G did not believe they needed to scan the classified workstations for vulnerabilities because the workstations did not connect to the corporate network or the Internet and because the workstations were inspected annually by the Defense Security Service to verify compliance with DoD 5220.22-M. Additionally, Contractor E did not always scan classified workstations that contained ballistic missile defense system technical information. Contractor E scanned the workstations that connected to the MDA's secure classified network but did not scan other workstations that contained classified ballistic missile defense system technical information. Without a process to identify and mitigate vulnerabilities on workstations, the contractors exposed workstations, including those workstations not connected to the network, to disgruntled employees who could potentially connect an infected device to the workstation and execute malicious activities.

The DoD OIG made multiple recommendations, including that the MDA Director for Acquisition include penalty clauses in awarded contracts to levy monetary sanctions on contractors that failed to implement physical and logical controls for protecting classified and unclassified ballistic missile defense system technical information. The MDA Director, responding for the MDA Director for Acquisition, disagreed, stating that the MDA would not focus on punishing contractors financially but on strengthening network protections and business practices for improving information protection. The Director stated that a "liquidated damages" clause would be more appropriate than imposing fines for noncompliant contractors, which he stated would be counterproductive to the MDA's goal of protecting unclassified controlled technical information. However, the Director stated that the MDA was working with contractors to ensure that preliminary controls were in place to protect ballistic missile defense system technical information and that the MDA would continue to assess when and how to use penalty clauses, award fees, and incentive fees as a way to encourage future compliance with DoD policy. The DoD OIG stated that the comments from the MDA Director did not address the specifics of the recommendation. The DoD OIG considered all six recommendations to the report unresolved because the

MDA Director disagreed with three of them and did not address the specifics of the remaining three. As of September 30, 2018, all six recommendations remained open.

AFAA Report No. F2018-00004-O10000, "Social Media," December 22, 2017

The AFAA found that Air Force personnel did not obtain proper approval to operate and monitor social media sites to prevent information or operational security violations. Specifically, none of the 258 sites approved by unit commanders were monitored for information or operational security concerns while all Public Affairs approved sites were monitored. This occurred because the Office of the Secretary of the Air Force Public Affairs did not develop a standard repeatable process for the establishment, tracking, and operation of official Air Force social media sites. Control and monitoring of official Air Force social media is essential to preventing compromise of information or operational security information.

The AFAA made several recommendations, including that the Secretary of the Air Force Public Affairs develop a standard repeatable process for the establishment, tracking, and operation of official Air Force social media sites. The Secretary of the Air Force Public Affairs concurred with the intent of the recommendations and agreed that corrective action was needed. The Secretary of the Air Force Public Affairs planned to develop the standard repeatable process for the approval, establishment and tracking of official Air Force social media sites. The AFAA considered the recommendations resolved; as of September 30, 2018, however, the four recommendations to the Secretary of the Air Force Public Affairs remained open.

Security Continuous Monitoring Category Takeaways

As discussed in the examples above, these six reports identified weaknesses in the category of Security Continuous Monitoring, such as contractors that did not scan workstations that stored classified ballistic missile defense system technical information to identify vulnerabilities. Air Force personnel also did not have proper approval to operate and monitor social media sites to prevent operational security violations. As a result, the DoD needs to ensure that officials monitored networks to detect potential cybersecurity events and perform the appropriate vulnerability scans.

Detection Processes Category

We identified one unclassified report addressing the Detection Processes category. The Framework defines Detection Processes category outcomes as those that should be maintained and tested to allow an organization to ensure that it is aware of anomalous events. The following report describes how detection processes affect DoD operations and noted that the DMDC made improvements in its use of host-based intrusion detection systems.

DoD OIG Report No. DODIG-2018-096, "Follow-Up Audit: The Defense Enrollment Eligibility Reporting System Security Posture," March 30, 2018

~~(FOUO)~~ [redacted] In this follow-up audit, the DoD OIG assessed the DMDC's implementation of the corrective actions to verify whether they addressed the identified issues.

Respond Function

We identified one unclassified report addressing the Respond function that identified risks in the Communications category. The Respond function includes those activities that assist the organization to develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The following section provides a summary of the report identified that addressed one of the five Framework categories under the Respond function—Communications.

To address cybersecurity risk in the Respond function, DoD needs controls and plans in place such as a response plan that supports the ability to contain the impact of a potential cybersecurity incident. The NIST Cybersecurity Framework provides standards and guidelines such as NIST Special Publications and other common practices that can be implemented to achieve the outcomes associated with each subcategory of the Respond function.

Communications Category

We identified one unclassified report addressing the Communications category. The Framework defines Communications category outcomes as those that allow an organization to coordinate its response activities with internal and external stakeholders. The following report describes how communication under the Respond function affects DoD operations.

[redacted]

~~(FOUO)~~ [redacted]

~~(FOUO)~~ [redacted]

Recover Function

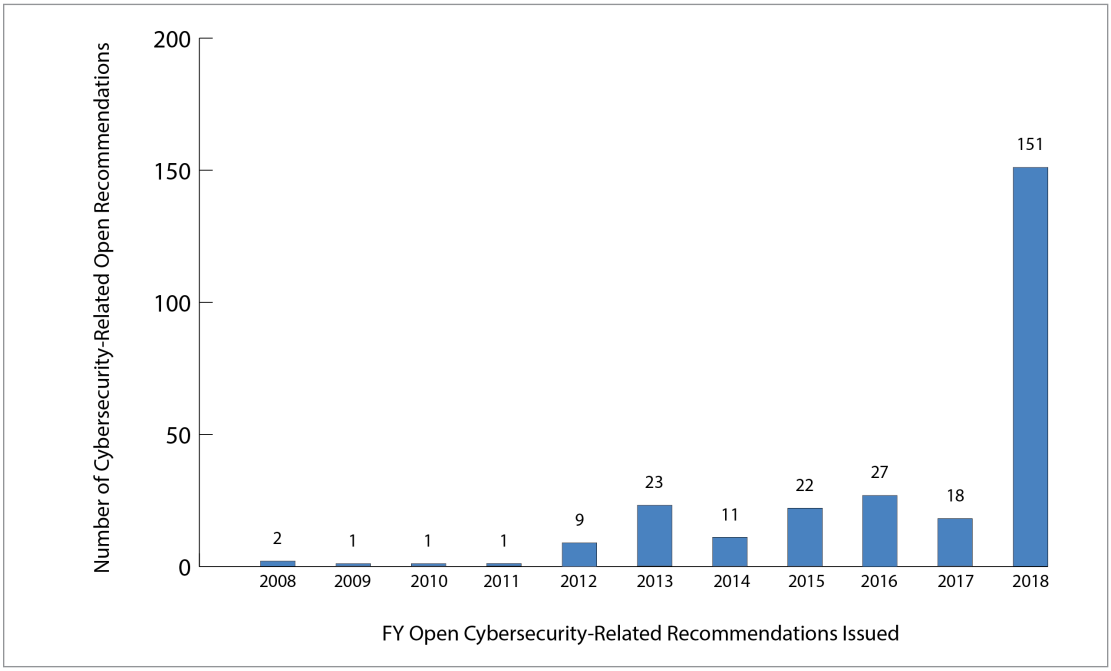
We did not identify any unclassified issued reports by the DoD oversight community and GAO between July 1, 2017 and June 30, 2018, pertaining to the Recover function. The Recover function includes those activities that help an organization recover to normal operations, in a timely manner, to reduce the impact from a cybersecurity incident. The Recover function consists of three categories—recovery planning, improvements, and communications.

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

Open Cybersecurity-Related Recommendations

As of September 30, 2018, we identified that the DoD needs to take action to close 266 open DoD cybersecurity-related recommendations—255 unclassified and 11 classified—from reports dating as far back as 2008. For example, the NAVAUDSVC had two recommendations that remain open for 10 years.[24] The AFAA had two recommendations that remained open for over 8 years—one from a 2009 report and one from a 2010 report.[25] The GAO and the DoD OIG each had recommendations dating back to reports issued in 2012. The figure shows the age of all open cybersecurity-related recommendations by fiscal year of report issuance.

Figure. Open Cybersecurity-Related Recommendations by Fiscal Year



Note: We acknowledge that 2018 recommendations were recently issued and, therefore, management did not have time to implement all actions to close the recommendations.

Source: The DoD OIG.

[24] NAVAUDSVC report as of September 30, 2018, "Information Security within the Marine Corps," February 20, 2008. Specifically, the NAVAUDSVC recommended that the Commandant of the Marine Corps execute annual testing and training for the contingency of operations plan and retain documentation of the testing as well as establish alternate sites to meet the Secretary of the Navy requirements.

[25] The AFAA recommendations included revising requirements in Air Force guidance and incorporating Chief Financial Officer compliance tracking for systems into a repository.

Recommendation Status for Reports Included in this Year's Summary Report

The DoD oversight community and the GAO made 175 recommendations in 20 unclassified and 4 classified reports issued between July 1, 2017, and June 30, 2018. Of the 175 recommendations, 151 remained open as of September 30, 2018, with the majority of the recommendations in the Identify and Protect functions. For example, the DoD OIG had 36 open recommendations from Report No. DODIG-2018-109 relating to the Identity Management and Access Control category under the Protect function.[26] See Appendix F for a matrix of open recommendations from unclassified reports by NIST Cybersecurity Framework category.

Additionally, the majority of the 151 recommendations that remained open as of September 30, 2018 were resolved. However, 39 of the recommendations were unresolved.[27] Specifically, the DoD:

- partially agreed with 6 recommendations,
- provided actions that partially addressed the identified issues for 25 recommendations,
- disagreed with 4 recommendations, and
- did not provide a response for 4 recommendations.

For example, the DoD partially concurred with a recommendation made in Report No. GAO-18-47 to update the DoD's cyber incident coordination training to incorporate the tenets of the Presidential Policy Directive on United States Cyber Incident Coordination (referred to as PPD-41). The DoD acknowledged the need to continue its emphasis on cyber incident coordination training and stated that the DoD was committed to updating the appropriate training as part of its formal after action reviews during each exercise and training event. The DoD further stated that it prepares for cyber incidents by exercising interagency roles and responsibilities, and command and control within a cyber threat scenario. In response, the GAO stated that, while these exercises emphasize the development of comprehensive cyber incident response plans and seek to foster cyber incident coordination, the DoD did not identify any specific exercise or training event in which the DoD will incorporate the tenets of PPD-41 and thus, GAO believes that this recommendation is still open.

[26] DoD OIG Report No. DODIG-2018-109, "Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities," May 2, 2018. The DoD OIG made recommendations that related to the Identity Management and Access Control category such as requiring the CIOs for the DHA, U.S. Army Medical Command, and military treatment facilities implement configuration changes to enforce the use of CACs when accessing DoD EHR systems and Army-specific systems, and configure passwords for the DoD EHR systems and Army-specific systems to meet DoD complexity requirements.

[27] The recommendations addressed here were unresolved at the time the reports were issued. They may have been resolved at a later date.

Appendix A

Scope and Methodology

We conducted this summary work from May 2018 through December 2018. This summary report supports the DoD OIG response to the annual independent assessment as required by FISMA. We followed generally accepted government auditing standards except for the standards of planning and evidence because the report summarizes previously released reports. Additionally, the July 12, 2018, Naval Audit Service peer review identified a potential threat to audit independence due to the Department of Navy organizational structure in effect during the period from March 13, 2013, through December 4, 2017. This alignment did not comply with generally accepted government auditing standards and the Department of the Navy policy regarding independence.

For this summary, we identified 20 unclassified and 4 classified reports that were issued by the DoD oversight community and the GAO from July 1, 2017, through June 30, 2018. Specifically, we coordinated with members of the Defense Council on Integrity and Efficiency Information Technology Committee, the intelligence community agencies, and the GAO to obtain the unclassified reports in this summary and classified reports in Appendixes G and H. We reviewed the findings and recommendations in each report and compared them against the five NIST Cybersecurity Framework function outcomes to determine if the findings and recommendations related to the NIST Framework. We also compared the findings and recommendations to the IG FISMA Reporting Metrics and summarized those in Appendix C. We did not review the supporting documentation for any of the reports. Because the summarized reports contained recommendations related to the identified cybersecurity weaknesses, this summary report does not contain additional recommendations. We prepared two appendixes to this report for information on classified reports issued during the time period.

Use of Computer-Processed Data

We did not use computer-processed data to perform this project.

Prior Coverage

During the last 5 years, the DoD OIG issued five reports summarizing cybersecurity weaknesses identified in 121 audit reports and 4 testimonies issued by the DoD audit community and the GAO. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/reports.html/.

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

DoD OIG

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

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

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

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

Report No. DODIG-2013-141, "DoD Information Assurance Weakness as Reported by Audit Reports Issued From August 1, 2012, Through July 31, 2013," September 30, 2013 ~~(Report is FOUO)~~

Appendix B

Unclassified Reports Issued Between July 1, 2017 and June 30, 2018

GAO

1. Report No. GAO-18-466, "Cybersecurity Workforce: Agencies Need to Improve Baseline Assessments and Procedures for Coding Positions," June 14, 2018
2. Report No. GAO-18-324, "Missile Defense: The Warfighter and Decision Makers Would Benefit from Better Communications about the System's Capabilities and Limitations," May 30, 2018
3. Report No. GAO-18-130, "Defense Business Systems: DoD Needs to Continue Improving Guidance and Plans for Effectively Managing Investments," April 16, 2018
4. Report No. GAO-18-211, "Critical Infrastructure Protection: Additional Actions Are Essential for Assessing Cybersecurity Framework Adoption," February 15, 2018
5. [redacted]
6. Report No. GAO-18-47, "Defense Civil Support: DoD Needs to Address Cyber Incident Training Requirements," November 30, 2017
7. Report No. GAO-17-512, "Defense Cybersecurity: DoD's Monitoring of Progress in Implementing Cyber Strategies Can Be Strengthened," August 1, 2017

DoD OIG

8. Report No. DODIG-2018-109, "Protection of Patient Health Information at Navy and Air Force Military Treatment Facilities," May 2, 2018 ~~(Report is FOUO)~~
9. Report No. DODIG-2018-096, "Followup Audit: The Defense Enrollment Eligibility Reporting System Security Posture," March 30, 2018 ~~(Report is FOUO)~~
10. [redacted]

11. Report No. DODIG-2018-094, "Logical and Physical Access Controls at Missile Defense Agency Contractor Locations," March 29, 2018
12. [redacted]
13. Report No. DODIG-2017-085, "Protection of Electronic Patient Health Information at Army Military Treatment Facilities," July 6, 2017 ~~(Report is FOUO)~~

Naval Inspector General

14. [redacted]

Naval Audit Service

15. [redacted]
16. [redacted]

Air Force Audit Agency

17. Report No. F2018-0005-O10000, "Electronic Records Cyber Hygiene," December 27, 2017
18. Report No. F2018-0004-O10000, "Social Media," December 22, 2017
19. Report No. F2018-0003-O10000, "Cybersecurity Program Management Configuration," December 22, 2017
20. Report No. F2018-0002-O10000, "Air Force Information Network (AFIN) and Air Force Network (AFNET) Data Call Validation," November 8, 2017
21. Report No. F2018-0001-O10000, "Wireless Network," October 10, 2017
22. [redacted]
23. Report No. F2017-0009-O10000, "Financial Systems Authority to Operate," September 20, 2017

Defense Contract Management Agency

24. Report No. DCMA-DMI-2017-001, "Audit of Cybersecurity Workforce Management," July 26, 2017

Appendix C

IG FISMA Reporting Metrics

FISMA requires each agency to conduct an annual independent evaluation to determine the effectiveness of the agency's information security program and practices. For an agency with an Inspector General (IG) appointed under the IG Act of 1978, that IG, or an independent external auditor designated by that IG, must perform the annual independent evaluation. The evaluation may be based in whole or in part on an audit, evaluation, or report relating to agency programs or practices. The agency head must report the results of the annual independent evaluation to the Office of Management and Budget. We plan to use this summary report to support the annual DoD IG independent evaluation and reporting requirement, which we are required to submit by October 31st of each year.

The FY 2018 IG FISMA Reporting Metrics provide reporting requirements across key areas to be addressed in the independent evaluation of agency information security programs. The FY 2018 IG FISMA Reporting Metrics were developed as a collaborative effort between the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal CIO Council. According to the Reporting Metrics, it represents a continuation of work that began in FY 2016 to align the IG metrics with the five functions from the NIST Cybersecurity Framework.

The FY 2018 IG FISMA Reporting Metrics include one update from the FY 2017 reporting metrics. Specifically, the Data Protection and Privacy metric was added to the 2018 reporting metrics, changing the total number of metrics from seven to eight. Table 9 provides a brief description of each FY 2018 IG FISMA Reporting Metric.

Table 9. FY 2018 IG FISMA Reporting Metrics

Metric	Description
Risk Management	Program and supporting processes for managing threats to organization operations, assets, and individuals. Includes assessing, responding to, and monitoring of risk over time.
Configuration Management	Collection of activities focused on establishing and maintaining the integrity of information technology products and information systems. Includes control of processes for initializing, changing, and monitoring the configurations of those products and systems.
Identity and Access Management	Processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources.
Data Protection and Privacy	Safeguards used to protect sensitive information about individuals.
Security Training	Formal activities, products, and services intended to create or enhance an individual's security knowledge or skills.
Information Security Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Incident Response	Mitigations of violations of security policies and recommended practices, also referred to as incident handling.
Contingency Planning	Policy and procedures used to guide the response to a perceived loss of mission capability.

Source: FY 2018 IG FISMA Reporting Metrics.

The IG FISMA Reporting Metrics state that alignment with the NIST Cybersecurity Framework helps promote consistent and comparable metrics and criteria in the CIO and IG metric processes while providing agencies with a meaningful independent assessment of the effectiveness of their information security program. Table 10 provides the eight FY 2018 IG FISMA Reporting Metrics and their alignment to the five NIST Cybersecurity Framework functions.

*Table 10. Comparison of the NIST Framework and FY 2018 IG FISMA Reporting Metrics**

Cybersecurity Framework Functions	FY 2018 IG FISMA Reporting Metrics
Identify	Risk Management
Protect	Configuration Management
Protect	Identity and Access Management
Protect	Data Protection and Privacy
Protect	Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

* The Contingency Planning metric also includes questions on planning and testing that apply to the Protect function.

Source: FY 2018 IG Reporting Metrics.

Risks by IG FISMA Reporting Metrics

We identified 20 unclassified and 4 classified reports issued by the DoD oversight community and the GAO between July 1, 2017, and June 30, 2018, that relate to the FY 2018 IG FISMA Reporting Metrics. Table 11 provides a summary of unclassified reports by FY 2018 IG FISMA Reporting Metric.

Table 11. Unclassified Reports by FY 2018 IG FISMA Reporting Metrics

Metric	GAO	DoD OIG	Navy	Air Force	DCMA	Other	Total
Risk Management	4	4	-	4	1	1	**14**
Configuration Management	1	4	-	-	-	-	**5**
Identity and Access	-	4	1	1	-	-	**6**
Data Protection and Privacy	-	4	2	-	-	1	**7**
Security Training	1	-	1	1	1	1	**5**
Information Security Continuous Monitoring	-	1	-	3	-	1	**5**
Incident Response	1	1	-	-	-	-	**2**
Contingency Planning	1	-	-	1	-	1	**3**

Note: Totals do not equal the number of reports identified because one report may cover more than one metric.

Source: The DoD OIG.

Appendix D

Matrix of Unclassified Reports Issued Between July 1, 2017, and June 30, 2018, by NIST Cybersecurity Framework Category

Agency Report No.	NIST Cybersecurity Framework														
	Identify Function Category						Protect Function Category						Detect Function Category		
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes
Government Accountability Office															
GAO-18-466	X		X					X							
GAO-18-324										X					
GAO-18-130		X													
GAO-18-211			X												
GAO-18-47	X	X	X							X					
GAO-17-512	X	X	X	X						X					
DoD Inspector General															
DODIG-2018-109	X			X			X		X	X		X			
DODIG-2018-096	X		X	X		X	X	X	X	X	X	X		X	X
DODIG-2018-094			X	X		X	X		X	X		X		X	
DODIG-2017-085	X			X			X		X	X		X			

Agency Report No.	NIST Cybersecurity Framework													
	Identify Function Category						Protect Function Category						Detect Function Category		
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes
Naval Inspector General															
[redacted]			X	X		X		X		X				X	
Naval Audit Service															
[redacted]			X				X	X							
[redacted]			X				X		X						
Air Force Audit Agency															
F2018-0005-O10000			X							X					
F2018-0004-O10000	X		X	X				X						X	
F2018-0003-O10000			X							X					
F2018-0002-O10000	X		X												
F2018-0001-O10000	X		X	X			X							X	
F2017-0009-O10000			X	X											
Defense Contract Management Agency															
DCMA-DMI-2017-001	X		X					X							
TOTALS	**10**	**3**	**16**	**9**	**0**	**3**	**7**	**6**	**5**	**10**	**1**	**4**	**0**	**5**	**1**

Note: The matrix does not include the Respond function because only one report addressed this area and is summarized in the body of the report or the Recover function because there were no reports issued that addressed this area.

Source: The DoD OIG.

Appendix E

Matrix of Unclassified Reports Issued Between July 1, 2017, and June 30, 2018, by IG FISMA Reporting Metric

Agency Report No.	FY 2018 IG FISMA Reporting Metrics							
	Risk Management	Configuration Management	Identity and Access Management	Data Protection and Privacy	Security Training	Information Security Continuous Monitoring	Incident Response	Contingency Planning
Government Accountability Office								
GAO-18-466					X			
GAO-18-324	X	X						
GAO-18-130	X							
GAO-18-211	X							
GAO-18-47							X	
GAO-17-512	X							X
DoD Inspector General								
DODIG-2018-109	X	X	X	X				
DODIG-2018-096	X	X	X	X			X	
DODIG-2018-094	X	X	X	X		X		
DODIG-2017-085	X	X	X	X				
Naval Inspector General								
[redacted]	X			X	X	X		X
Naval Audit Service								
[redacted]			X	X	X			
[redacted]				X				
Air Force Audit Agency								
F2018-0005-O10000								X
F2018-0004-O10000	X				X	X		
F2018-0003-O10000	X							

Agency Report No.	FY 2018 IG FISMA Reporting Metrics							
	Risk Management	Configuration Management	Identity and Access Management	Data Protection and Privacy	Security Training	Information Security Continuous Monitoring	Incident Response	Contingency Planning
F2018-0002-O10000	X							
F2018-0001-O10000	X		X			X		
F2017-0009-O10000						X		
Defense Contract Management Agency								
DCMA-DMI-2017-001	X				X			
TOTALS	**14**	**5**	**6**	**7**	**5**	**5**	**2**	**3**

Source: The DoD OIG.

Appendix F

Matrix of Open Recommendations in Unclassified Reports Issued Between July 1, 2017, and June 30, 2018, by NIST Cybersecurity Framework Function Category

Agency Report No.	NIST Cybersecurity Framework														
	Identify Function Category						Protect Function Category						Detect Function Category		
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes
Government Accountability Office															
GAO-18-466			2					2							
GAO-18-324										2					
GAO-18-130		1													
GAO-18-211			1												
GAO-18-47		1	1							2					
GAO-17-512			2												
DoD Inspector General															
DODIG-2018-109	7			2			31		10	10		5			
DODIG-2018-096	1						2				1	1		1	

Agency Report No.	NIST Cybersecurity Framework														
	Identify Function Category						Protect Function Category						Detect Function Category		
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes
DODIG-2018-094				1		6	4		4	5		4		2	
DODIG-2017-085	4			1			21		5	5		3			
Naval Inspector General															
[redacted]															
Naval Audit Service															
[redacted]			1				2	1							
[redacted]							1		2						
Air Force Audit Agency															
F2018-0005-O10000			3							3					
F2018-0004-O10000	3		2	3				1						3	
F2018-0003-O10000															
F2018-0002-O10000	3		1												
F2018-0001-O10000				1										1	
F2017-0009-O10000															

Agency Report No.	NIST Cybersecurity Framework														
	Identify Function Category						Protect Function Category						Detect Function Category		
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy	Supply Chain Risk Management	Identity Management and Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology	Anomalies and Events	Security Continuous Monitoring	Detection Processes
Defense Contract Management Agency															
DCMA-DMI-2017-001	4							2							
TOTALS	**22**	**2**	**17**	**8**	**0**	**6**	**61**	**6**	**21**	**27**	**1**	**13**	**0**	**7**	**0**

Source: The DoD OIG.

Appendix G

Secret Reports Issued Between July 1, 2017 and June 30, 2018

This appendix contains information about classified reports and how each report relates to the NIST Cybersecurity Framework. To request access to this appendix, please file a Freedom of Information Act (FOIA) request online at http://www.dodig.mil/FOIA/Submit-FOIA.

Appendix H

Top Secret Reports Issued Between July 1, 2017 and June 30, 2018

This appendix contains information about classified reports and how each report relates to the NIST Cybersecurity Framework. To request access to this appendix, please file a Freedom of Information Act (FOIA) request online at http://www.dodig.mil/FOIA/Submit-FOIA.

Acronyms and Abbreviations

AFAA	Air Force Audit Agency
CAC	Common Access Card
CIO	Chief Information Officer
DCMA	Defense Contract Management Agency
DHA	Defense Health Agency
DMDC	Defense Manpower Data Center
EHR	Electronic Health Record
FISMA	Federal Information Security Modernization Act of 2014
GAO	Government Accountability Office
MDA	Missile Defense Agency
NIST	National Institute of Standards and Technology
NAVAUDSVC	Naval Audit Service

Whistleblower Protection
U.S. Department of Defense

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

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

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

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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