Report No. DODIG-2018-126

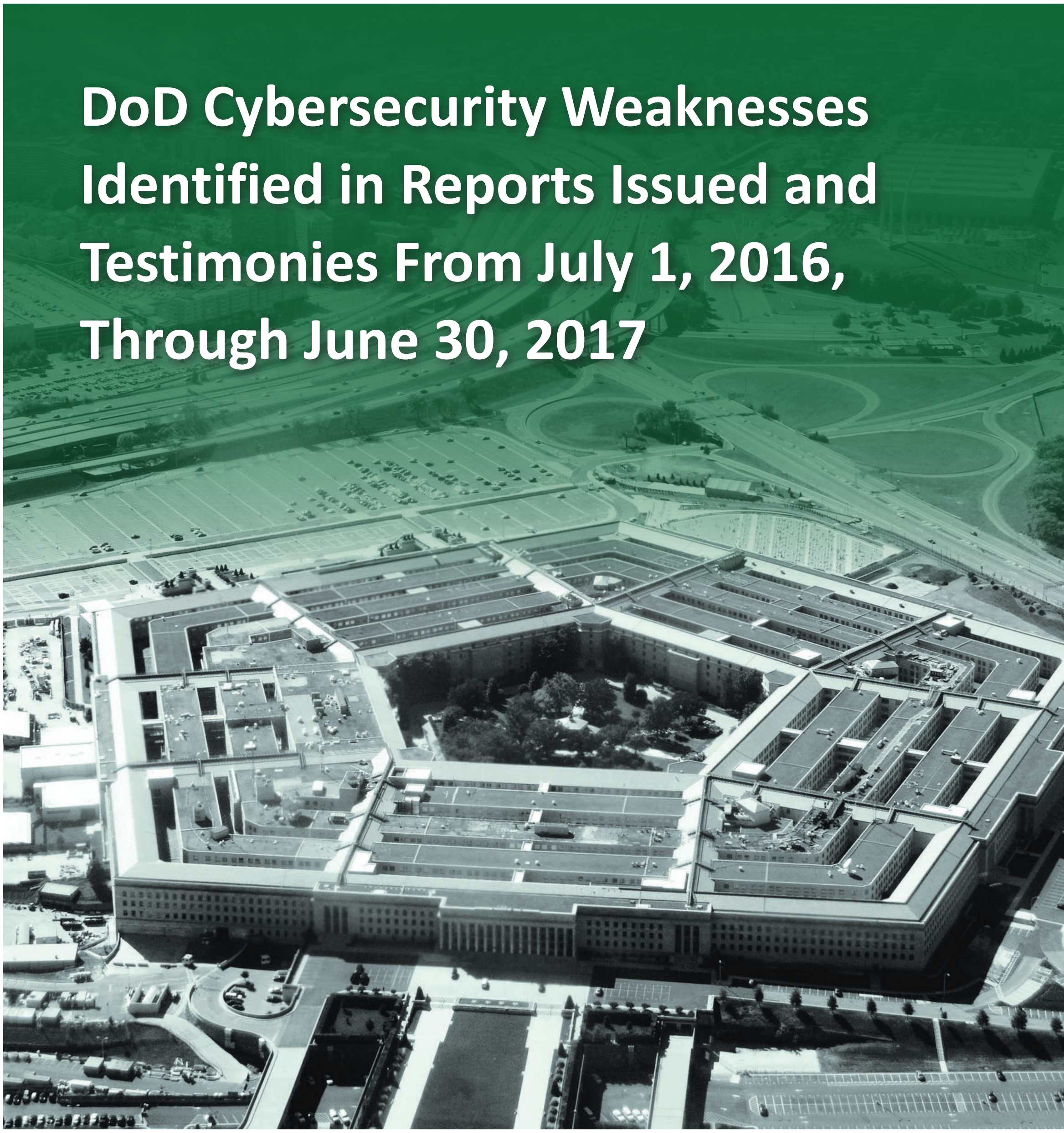
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

JUNE 13, 2018

DoD Cybersecurity Weaknesses Identified in Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017



INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

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

~~FOR OFFICIAL USE ONLY~~

Results in Brief

DoD Cybersecurity Weaknesses Identified in Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017

June 13, 2018

Objective

Our objective was to categorize and summarize cybersecurity weaknesses identified in unclassified reports issued and testimonies given by members of the DoD oversight community and the Government Accountability Office (GAO) between July 1, 2016, and June 30, 2017. Specifically, we categorized and summarized reports and testimonies by:

- the five functions identified in the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014 (NIST Cybersecurity Framework), which is designed to help owners and operators of critical infrastructure identify, assess, and manage cyber risk; and
- the seven "FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics," which are designed to determine the effectiveness of an agency's information security program and practices.

Summary

Cybersecurity is critical to DoD operations; however, cybersecurity remains a significant challenge for the DoD. Executive Order 13800 mandates that agencies use the NIST Cybersecurity Framework to manage cybersecurity risk. The five functions in the NIST Cybersecurity Framework Core also provide a strategic view of cybersecurity risk management.

Summary (cont'd)

In summarizing 29 unclassified reports and 1 unclassified testimony issued by the DoD oversight community and GAO between July 1, 2016, and June 30, 2017, we determined that the DoD still faces challenges in key cybersecurity risk areas pertaining to Identify, Protect, and Detect functions. These three functions are designed to help an organization to understand its cybersecurity risks, implement appropriate safeguards, and identify cybersecurity events. Specifically, the reports we reviewed identified:

- weaknesses in establishing or maintaining inventories for information systems, hardware, and software licenses;
- weaknesses in system account and password management as well as in physical access to information technology assets;
- weaknesses in vulnerability and configuration management as well as incident response testing and continuity planning and testing; and
- weaknesses in the Security Continuous Monitoring and Detection Processes categories of the Detect function. Security continuous monitoring of information systems is used to identify cybersecurity events while detection processes are used to ensure timely and adequate awareness of anomalous events.

In addition to summarizing the reports and aligning them within the NIST Cybersecurity Framework, we also reviewed the reports to identify findings relevant to the IG FISMA Reporting Metrics. FISMA requires each federal agency to develop, document, and implement an Agency-Wide information security program to protect the information and information systems supporting agency operations and assets. FISMA also requires federal IGs to conduct an annual independent evaluation to determine the effectiveness of the

Summary (cont'd)

agency's information security program and practices and report the results to the Office of Management and Budget.[1] We used the summarized findings and recommendations when developing this report to support the DoD IG annual independent evaluation and reporting requirement, which we communicated to the DoD Chief Information Officer on October 31, 2017.

Of the 29 unclassified reports and 1 unclassified testimony we reviewed, we identified 26 reports that identified DoD weaknesses associated with the seven FY 2017 IG FISMA Reporting Metrics. The metrics with the most frequent weaknesses identified in the reports were the Risk Management, Identity and Access Management, and Configuration Management metrics. The 26 reports are a subset of the 29 reports that pertained to the NIST Cybersecurity Framework functions, and the most pervasive DoD cybersecurity weaknesses are discussed in the first paragraph of this Summary.

To help ensure that the DoD provides adequate oversight of the DoD risks pertaining to the NIST Cybersecurity Framework and the IG FISMA Reporting Metrics, we plan to discuss the results of this DoD cybersecurity summary project at future meetings of the Defense Council on Integrity and Efficiency (DCIE) Information Technology Committee and use these results in planning reviews of cybersecurity by DoD oversight organizations.[2] Finally, we also intend to include classified reports in future cybersecurity summary reviews to provide a fuller summary of oversight of DoD cybersecurity activities.

[1] For an agency with an 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.

[2] The DCIE is a coordination and cooperation group chaired by DoD OIG which includes members from the DoD oversight community, such as representatives from the Defense agencies and the internal audit, inspection, and investigative organizations of the military departments. The DCIE Information Technology Committee, one of six DCIE committees, meets regularly to discuss oversight of DoD information technology and cyber related issues.

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

June 13, 2018

MEMORANDUM FOR DOD 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: DoD Cybersecurity Weaknesses Identified in Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017 (Report No. DODIG-2018-126)

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

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

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

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

Contents

Contents (cont'd)

Introduction

Objective

Our objective was to categorize and summarize cybersecurity weaknesses identified in unclassified reports issued and testimonies by members of the DoD oversight community and the Government Accountability Office (GAO) between July 1, 2016, and June 30, 2017. 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 reports and testimonies summarized in this report.

Background

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 will 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 or assets."

This summary report is divided into two sections that provide insight into the effectiveness of the DoD Cybersecurity Program.

- Section I categorizes and summarizes reports issued and testimonies made by the functions identified in the National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity," February 12, 2014 (NIST Cybersecurity Framework).
- Section II categorizes and summarizes reports issued and testimonies made by the metrics identified in the "FY 2017 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics" (FY 2017 IG FISMA Reporting Metrics).

NIST Cybersecurity Framework

On February 12, 2013, the President of the United States signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." Executive Order 13636 calls for the development of a voluntary cybersecurity framework that provides a prioritized, flexible, repeatable, performance-based, and cost effective approach to help owners and operators of critical infrastructure identify, assess, and manage cyber risk. The resulting NIST Cybersecurity Framework was created through collaboration between Government and private sector entities.

The NIST Cybersecurity Framework is composed of three parts: the Core, the Implementation Tiers, and the Profiles. The Core provides a set of cybersecurity activities and desired outcomes that are common across critical infrastructure sectors. The Implementation Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics described in the NIST Cybersecurity Framework. Finally, the Profiles represent the outcomes based on business needs that an organization has selected from the NIST Cybersecurity Framework. The Core represents a common set of activities for cybersecurity risk management that can be used to categorize cybersecurity weaknesses. When considered together, the five functions in the Core—Identify, Protect, Detect, Respond, and Recover, provide a strategic view of the risk management lifecycle.[3] Table 1 contains a description of the five functions.

Table 1. NIST Cybersecurity

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

Source: NIST Cybersecurity Framework.

Each function is subdivided into categories consisting of cybersecurity outcomes tied to programmatic needs and particular activities. There are a total of 22 categories for the 5 functions. See Section I for a description of the categories by function.

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

[3] Although the Recover function description addresses maintaining plans for resilience, incident response and continuity plans are established and tested within the Protect function.

FISMA Evaluation

The purpose of FISMA is to provide a comprehensive framework to ensure the effectiveness of agency information security controls. FISMA requires each agency to develop, document, and implement an Agency-Wide information security program to protect the information and information systems supporting agency operations and assets. In addition, 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 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 used the summarized findings and recommendations when developing this report to support the DoD IG annual independent evaluation and reporting requirement, which we communicated to the DoD Chief Information Officer (CIO) on October 31, 2017.

The FY 2017 IG FISMA Reporting Metrics provide reporting requirements across key areas to be addressed in the independent evaluation of agency information security programs. The FY 2017 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 FY 2017 IG FISMA Reporting Metrics, the metrics represent a continuation of work started in FY 2016, when the IG reporting metrics were aligned with the five NIST Cybersecurity Framework functions. The FY 2017 reporting metrics state that the 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 2 shows the seven FY 2017 IG FISMA Reporting Metrics and their alignment to the five NIST Cybersecurity Framework functions. See Section II for a description of each metric.

Table 2. FY 2017 IG FISMA Reporting Metrics[4]

Cybersecurity Framework Functions	FY 2017 IG FISMA Reporting Metrics
Identify	Risk Management
Protect	Configuration Management
	Identity and Access Management
	Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

Source: FY 2017 IG FISMA Reporting Metrics.

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

Section I

Reports and Testimonies by NIST Cybersecurity Framework Function and Category

We categorized and summarized 29 unclassified reports issued and 1 testimony made by the DoD oversight community and the GAO, from July 1, 2016, through June 30, 2017, that collectively identified DoD weaknesses in 3 of the 5 functions and 13 of the 22 associated categories from the NIST Cybersecurity Framework. The 29 reports contained 161 recommendations to correct DoD weaknesses such as asset management and access controls related to the NIST Cybersecurity Framework. See Table 3 for the number of reports and testimonies by NIST Cybersecurity Framework function and category. See Appendices C and D for a matrix of reports by NIST Cybersecurity Framework Identify and Protect function categories. A matrix was not prepared for the Detect function since both reports are included in this section.

Table 3. Reports and Testimonies by NIST Cybersecurity Framework Function and Category

Function	Category	GAO	DoD OIG	Army	Air Force	Total
Identify	Asset Management	8	4	2	7	21
	Business Environment	3	0	0	0	3
	Governance	6	2	2	0	10
	Risk Assessment	2	0	2	1	5
	Risk Management Strategy	2	0	0	2	4
Protect	Access Control	0	3	1	5	9
	Awareness & Training	0	1	1	1	3
	Data Security	0	1	0	0	1
	Information Protection Processes & Procedures	4	3	3	1	11
	Maintenance	0	0	1	0	1
	Protective Technology	0	2	0	2	4
Detect	Anomalies & Events	0	0	0	0	0
	Security Continuous Monitoring	0	1	0	0	1
	Detection Processes	0	0	0	1	1

Function	Category	GAO	DoD OIG	Army	Air Force	Total
Respond	Response Planning	0	0	0	0	0
	Communications	0	0	0	0	0
	Analysis	0	0	0	0	0
	Mitigation	0	0	0	0	0
	Improvements	0	0	0	0	0
Recover	Recovery Planning	0	0	0	0	0
	Improvements	0	0	0	0	0
	Communications	0	0	0	0	0

Source: The DoD OIG.

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

Identify Function

We identified 25 reports and 1 testimony related to the Identify function. The NIST Cybersecurity Framework states that the Identify function refers to the development of the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables the organization to focus and prioritize its efforts in accordance with its risk management strategy and business needs. The categories in the Identify function are Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

- **Asset Management.** Data, personnel, devices, systems, and facilities are identified and managed to achieve business purposes consistent with business objectives and risk strategy. We identified 20 reports and 1 testimony with 40 recommendations addressing Asset Management.
- **Business Environment.** Mission, objectives, stakeholders, and actions are understood, prioritized, and used to inform cybersecurity roles, responsibilities, and risk management decisions. We identified three reports with nine recommendations addressing Business Environment.
- **Governance.** Policies, procedures, and processes to manage and monitor regulatory, legal, risk, environmental, and operational requirements are understood and used to inform cybersecurity risk management. We identified 9 reports and 1 testimony with 13 recommendations addressing Governance.

- **Risk Assessment.** Cybersecurity risk to operations (including mission, functions, image, or reputation), organizational assets, and individuals is understood. We identified 5 reports with 28 recommendations addressing Risk Assessment.
- **Risk Management Strategy.** Priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. We identified four reports with seven recommendations addressing Risk Management Strategy.

The following two reports are examples of how cybersecurity weaknesses in the Identify function affect DoD operations. Specifically, in the first report, Air Force Audit Agency (AFAA) determined that the Air Force needed to improve accountability for wireless assets to reduce exposure to loss, theft, tampering, and exploitation. In the second report, the GAO determined that DoD needed a strategy to conduct security assessments for its Joint Information Environment to determine the extent to which actual or proposed changes to the system or its environment will impact system security.

AFAA Report No. F2016-0005-O10000, "Air Forces Central Command Wireless Network Security," September 9, 2016

This report addressed the Asset Management category of the Identify function. The AFAA found that Expeditionary Communications Squadron information technology equipment custodians had not entered any of the 69 wireless access points installed at three air bases into the Air Force Equipment Management System–Asset Inventory Management. Furthermore, the AFAA observed that, during the audit, information technology equipment custodians did not find 3 of the 69 wireless access points listed on the Air Forces Central Command (AFCENT) Network Operations and Security Center accountability records. A wireless access point allows authorized computers to connect to the DoD network using radio signals. Wireless access points must be properly accounted for due to their capability to process and transmit sensitive information.

The wireless access points were not properly accounted for because AFCENT personnel did not coordinate the installation of wireless access points with appropriate installation personnel to ensure wireless access points were added to the Air Force Equipment Management System–Asset Inventory Management. In addition, information technology equipment custodians had not complied with existing guidance requiring them to perform inventories to verify that assets were on hand. Finally, AFCENT Network Operations and Security Center personnel did not follow up with installation personnel when wireless access points stopped appearing on the AFCENT Network Operations and Security Center wireless network controller.[5] Without visibility and control over wireless access points, AFCENT cannot manage assets vital to information security and protect them from loss, theft, tampering, and exploitation by hostile actors.

Without visibility and control over wireless access points, AFCENT cannot manage assets vital to information security and protect them from loss, theft, tampering, and exploitation by hostile actors.

The AFAA recommended that the Commander, AFCENT:

- develop a standard repeatable process requiring personnel to coordinate installation of wireless access points with appropriate installation personnel to ensure they are added to Air Force Equipment Management System–Asset Inventory Management; and
- implement internal control procedures to ensure that information technology equipment custodians comply with inventory requirements, and that Security Center personnel notify Expeditionary Communications Squadron personnel when wireless access points no longer appear on the AFCENT Network Operations and Security Center wireless network controller.

The Commander, AFCENT agreed with the recommendation to develop a standard repeatable process to coordinate wireless access point installation. The Commander stated they will develop the process and that equipment custodian officers will follow up to verify inclusion in the Air Force Equipment Management System–Asset Inventory Management. In addition, the Commander agreed with the intent of the recommendation to implement internal control procedures stating they will implement internal control procedures to ensure compliance with inventory requirements. Finally, the Commander stated that the AFCENT Network Operations and Security Center would work with Expeditionary Communications Squadron personnel to confirm access to the tool permitting them to monitor and manage their base wireless access point equipment.

GAO Report No. GAO-16-593, "Joint Information Environment: DoD Needs to Strengthen Governance and Management," July 14, 2016

This report addressed the Governance category of the Identify function. The GAO found that the DoD lacked a strategy to conduct Joint Information Environment security assessments required by Federal and DoD guidance. The Joint

[5] Wireless access points are capable of transmitting their status to Air Force Network Operations and Security Centers through a wireless network controller, which permits users to monitor the status of wireless devices. This capability allows a Network Operations and Security Center to conduct inventories remotely to identify these devices. In this case, wireless access points stopped appearing in the remote inventory.

Information Environment is a DoD initiative to consolidate information technology infrastructure to achieve savings and improve network security. According to the NIST, a security assessment should be conducted to determine the extent to which proposed or actual changes to an information system or its environment can affect the security of the system. To meet that requirement, the Joint Staff issued an order for U.S. Cyber Command (USCYBERCOM) to conduct a security assessment of Joint Information Environment plans, and later added a requirement to the order for the National Security Agency to conduct a security assessment of the Joint Information Environment security architecture.

The DoD CIO established a team, including USCYBERCOM and the National Security Agency, to review the Joint Information Environment security architecture. However, DoD CIO officials said that the team has not documented plans for completing the security assessment because testing and assessments are the responsibility of the Director, Operational Test and Evaluation, and the Joint Interoperability Test Command. However, the Director, Operational Test and Evaluation stated that preparation of plans for Joint Information Environment testing and assessments is the responsibility of the DoD CIO. Without a security assessment of Joint Information Environment or a plan to conduct an assessment, the DoD is limited in its ability to ensure early detection of security-related weaknesses and deficiencies and is hindered in achieving key goals, such as ensuring increased cyber security through the Joint Information Environment.

Without a security assessment of Joint Information Environment or a plan to conduct an assessment, the DoD is limited in its ability to ensure early detection of security-related weaknesses and deficiencies and is hindered in achieving key goals, such as ensuring increased cyber security through the Joint Information Environment.

The GAO recommended that the Secretary of Defense direct the DoD CIO, and other entities as appropriate, to develop a strategy for conducting Joint Information Environment security assessments. The strategy should describe the resources needed to execute the strategy, responsible organizations, and a schedule to complete the assessments. The Principal Deputy DoD CIO partially agreed, stating that the team established to review the security architecture meets the recommendation requirement. However, the GAO maintained that the DoD did not address the need for a strategy or a schedule. Without a strategy that identifies the resources needed to execute the strategy, the responsible organizations, and a schedule to complete the assessments, the GAO stated that the DoD lacks assurance that the required assessments will be completed.

Protect Function

We identified 18 reports related to the Protect function. The Protect function refers to the development and implementation of appropriate safeguards to ensure delivery of critical infrastructure services. The Protect function supports the ability to limit or contain the impact of a potential cybersecurity event. The categories in the Protect function are Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance, and Protective Technology.

- **Access Control.** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions. We identified 9 reports with 23 recommendations addressing Access Control.
- **Awareness and Training.** Personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements. We identified three reports with six recommendations addressing Awareness and Training.
- **Data Security.** Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information. We identified one report with two recommendations addressing Data Security.
- **Information Protection Processes and Procedures.** Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets. Security policies specifically address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities. We identified 11 reports with 67 recommendations addressing Information Protection Processes and Procedures.
- **Maintenance.** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. We identified one report with one recommendation addressing Maintenance.
- **Protective Technology.** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements. We identified four reports with seven recommendations addressing Protective Technology.

~~(FOUO)~~ The following two reports are examples of how cybersecurity weaknesses in the Protect function affect DoD operations. Specifically, in the first report [redacted]

[redacted].

[redacted][redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[7] On February 1, 2018, the Undersecretary of Defense for Acquisition, Technology, and Logistics reorganized into the Undersecretary of Defense for Research and Engineering and the Undersecretary of Defense for Acquisition and Sustainment.

[8] [redacted]

[redacted]

Detect Function

We identified two reports related to the Detect function. The Detect function refers to the development and implementation of activities to identify the occurrence of cybersecurity events. The categories in the Detect function are Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

- **Anomalies and Events.** Anomalous activity is detected in a timely manner and the potential impact of events is understood. We did not identify any reports addressing Anomalies and Events.
- **Security Continuous Monitoring.** Information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures. We identified one report with one recommendation addressing Security Continuous Monitoring.
- **Detection Processes.** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. We identified one report with two recommendations addressing Detection Processes.

~~(FOUO)~~ The following reports describe how cybersecurity weaknesses in the Detect function affect DoD operations. Specifically, in the first report, [redacted] In the second report, the AFAA determined that personnel for two medical systems needed to improve monitoring of system security incidents by implementing Federal standards for system controls contained in updated DoD guidance.

[redacted]

[redacted] [redacted] An authorization to operate is a DoD authorizing decision based on achieving and maintaining an acceptable risk posture for the system. The authorizing official grants the authorization to operate based on the level of risk to organizational operations. If overall risk is determined to be acceptable, and there are no noncompliant controls with a high or very high level of risk, a 3-year authorization to operate can be granted. If overall risk is determined to be acceptable due to mission criticality, but there are noncompliant controls with a high or very high level of risk, a 1-year authorization to operate with conditions can be granted by the authorizing official with permission of the responsible Component CIO. After the 1-year period, if noncompliant controls with a high or very high level of risk still exist, the authorizing official may again grant a 1-year authorization to operate with conditions only if the Component CIO grants permission. If the risk for the high or very high noncompliant controls is mitigated to an acceptable risk level, a full 3-year authorization to operate can be granted.

~~(FOUO)~~ The report states that the authorizing official did not grant a 3-year authorization to operate because he identified noncompliant controls with a high and very high level of risk. For example, [redacted] [redacted]

[9] [redacted]

[redacted]

AFAA Report No. F2016-0004-O10000, “Medical Systems – General and Application Controls,” September 9, 2016

This report addressed the Detection Processes category of the Detect function. The AFAA found that Composite Health Care System and Defense Medical Logistics Standard Support management personnel did not establish local procedures to monitor system security incidents at 9 of 11 locations. The AFAA determined that procedures were not established because Composite Health Care System and Defense Medical Logistics Standard Support personnel did not implement the NIST Risk Management Framework. Further, personnel did not categorize system risk, select and implement appropriate controls, or assess those general and application controls required by NIST and the Federal Information Security Management Act. Instead, Composite Health Care System and Defense Medical Logistics Standard Support personnel followed pre-2014 DoD 8500-series policies that did not reflect current Federal regulations for general and application controls.[10] The report stated that the information system control discrepancies cast doubt on the reliability of medical operations data used to administer care to beneficiaries and manage medical materiel. In addition, the Composite Health Care System and the Defense Medical Logistics Standard Support system provide information affecting the Air Force financial statements. Therefore, if independent public accountants cannot rely on the system of internal controls supporting Air Force financial statements, they will have to increase substantive testing sample sizes and increase the cost of audit accordingly.

The AFAA recommended that the Air Force Surgeon General, in coordination with the Defense Health Agency and Air Force CIO, direct Composite Health Care System and Defense Medical Logistics Standard Support program managers to implement Federal NIST system control standards contained in the updated risk

[10] These policies included DoD Directive 8500.01E, “Information Assurance,” April 23, 2007, DoD Instruction 8500.2, “Information Assurance Implementation,” February 6, 2003, and DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process,” November 28, 2007.

management framework-DoD Instruction 8510.01.[11] The Air Force Surgeon General agreed to coordinate on requirements for NIST system controls, and subsequently direct program management personnel to implement appropriate standards in the updated DoD instruction. Furthermore, the AFAA recommended that the Air Force Surgeon General establish an internal control process to validate compliance with Federal NIST system control standards contained in the updated DoD Instruction 8510.01. The Air Force Surgeon General agreed to establish an internal control process to validate compliance with NIST system controls in the updated DoD instruction.

Respond Function

We did not identify any reports or testimonies related to the Respond function. The Respond function refers to the development and implementation of actions to take after a cybersecurity event is detected. The Respond function supports the ability to contain the impact of the event. The categories in the Respond function are Response Planning, Communications, Analysis, Mitigation, and Improvements.

- **Response Planning.** Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events. We did not identify any reports addressing Response Planning.
- **Communications.** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies. We did not identify any reports addressing Communications.
- **Analysis.** Analysis is conducted to ensure adequate response and support recovery activities. We did not identify any reports addressing Analysis.
- **Mitigation.** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident. We did not identify any reports addressing Mitigation.
- **Improvements.** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. We did not identify any reports addressing Improvements.

[11] DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014 establishes the DoD risk management framework to manage the life-cycle cybersecurity risk to DoD information technology and replaces the DoD Information Assurance Certification and Accreditation Process. The Instruction requires that DoD must establish and use a risk management framework, which includes and integrates DoD mission areas, to satisfy the Federal Information Security Management Act requirements.

Recover Function

We did not identify any reports or testimonies related to the Recover function. The Recover function refers to the development and implementation of activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity event. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. The categories in the Recover function are Recovery Planning, Improvements, and Communications.

- **Recovery Planning.** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events. We did not identify any reports addressing Recovery Planning.
- **Improvements.** Recovery planning and processes are improved by incorporating lessons learned into future activities. We did not identify any reports addressing Improvements.
- **Communications.** Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, and vendors. We did not identify any reports addressing Communications.

Summary

Cybersecurity risk management is critical in safeguarding DoD’s use of cyberspace to support its operations; however, cybersecurity remains a significant challenge for DoD. Executive Order 13800 mandates that agencies use the NIST Cybersecurity Framework to manage cybersecurity risk. The five functions in the NIST Cybersecurity Framework Core provide a strategic view of the risk management lifecycle. In summarizing 29 unclassified reports and 1 unclassified testimony issued by the DoD oversight community and GAO, we determined that the DoD still faces challenges in key cybersecurity risk areas pertaining to the Identify, Protect, and Detect functions. These three functions help an organization to understand its cybersecurity risks, implement appropriate safeguards, and identify cybersecurity events. Specifically, 25 reports and 1 testimony collectively addressed DoD weaknesses in the Identify function, primarily in the Asset Management category.

In summarizing 29 unclassified reports and 1 unclassified testimony issued by the DoD oversight community and GAO, we determined that the DoD still faces challenges in key cybersecurity risk areas pertaining to the Identify, Protect, and Detect functions.

Asset management allows an organization to identify and manage its resources, such as systems and devices, to accomplish business objectives. For example, the reports identified weaknesses in establishing or maintaining inventories for information systems, hardware, and software licenses. The reports generally recommended that DoD establish or update policies, processes, or controls to correct the inventory weaknesses.

Additionally, 18 reports collectively addressed DoD weaknesses in the Protect function, primarily in the Access Control and Information Protection Processes and Procedures categories. Access control limits asset and facility access to authorized users, processes, or devices while information protection processes and procedures are used to manage protection of information systems and assets. For example, the reports identified weaknesses in system account and password management as well as in physical access to information technology assets. In addition, the reports identified weaknesses in vulnerability and configuration management as well as incident response testing and continuity planning and testing. The reports generally recommended that DoD establish or update policies, processes, or controls to correct the weaknesses.

~~(FOUO)~~ Furthermore, two reports collectively addressed DoD weaknesses in the Security Continuous Monitoring and Detection Processes categories of the Detect function. Security continuous monitoring of information systems is used to identify cybersecurity events while detection processes are used to ensure timely and adequate awareness of anomalous events. [redacted] while the other report identified a weakness in establishing procedures to monitor security incidents and recommended that DoD implement updated guidance and establish associated controls to correct the weakness.

Finally, the Respond and Recover functions allow an organization to contain the impact of a cybersecurity event and return to normal operations in a timely manner. Although we did not identify any unclassified reports addressing these last two functions, the 29 reports and 1 testimony collectively addressing the first three functions demonstrate the importance of oversight to identify areas where DoD needs to improve its cybersecurity risk management. We recognize that the oversight community and GAO may have addressed the Respond and Recover functions in classified reports during the reporting period, however we did not summarize those here because we limited our review to unclassified reports. To help ensure that oversight resources are properly allocated to address DoD risks pertaining to the NIST Cybersecurity Framework, we plan to discuss the results of this DoD cybersecurity summary project at future meetings of the Defense Council on Integrity and Efficiency Information Technology Committee for use in their ongoing planning efforts.[12] We also plan to include classified reports in future cybersecurity summary projects to provide a broader view of oversight for DoD cybersecurity activities.

[12] The Defense Council on Integrity and Efficiency, a coordination and cooperation group chaired by DoD OIG, includes the DoD oversight community such as representatives from the Defense agencies as well as the internal audit, inspection, and investigative organizations of the military departments. The Information Technology Committee, one of the six Defense Council on Integrity and Efficiency committees, meets regularly to discuss oversight of DoD cyber issues.

Section II

Reports by FY 2017 IG FISMA Reporting Metrics

We categorized and summarized 29 unclassified reports and 1 testimony issued by the DoD oversight community and GAO, from July 1, 2016, through June 30, 2017. Of those reports and testimony, 26 reports identified DoD weaknesses in the seven FY 2017 IG FISMA Reporting Metrics.[13] The 26 reports contained 153 recommendations to correct DoD weaknesses such as risk management and configuration management related to the reporting metrics. See Table 4 for the number of reports by FY 2017 IG FISMA Reporting Metric. See Appendix E for a matrix of reports by FY 2017 IG FISMA Reporting Metric.

Table 4. Reports by FY 2017 IG FISMA Reporting Metric

FISMA Reporting Metric	GAO	DoD OIG	Army	Air Force	Total
Risk Management	6	5	2	8	21
Configuration Management	2	3	3	1	9
Identity and Access Management	1	3	1	5	10
Security Training	0	1	1	1	3
Information Security Continuous Monitoring	1	1	2	0	4
Incident Response	3	0	0	1	4
Contingency Planning	1	2	0	1	4

Source: The DoD OIG.
Note: Totals do not equal the number of reports and testimonies identified because one report may cover more than one IG FISMA Reporting Metric.

Risk Management

We identified 21 reports with 88 recommendations addressing risk management. Risk management is the process for managing threats to operations, assets, individuals, other organizations, and the Nation. Risk management includes assessing risk, responding to risk, and monitoring risk over time.

~~(FOUO)~~ The following two reports are examples of how cybersecurity weaknesses in risk management affect DoD operations. Specifically, in the first report, [redacted]

[13] The DoD oversight community and GAO issued three reports and one testimony that covered categories under the NIST Cybersecurity Framework, but not the IG FISMA Reporting Metrics. As a result, we only discuss 26 reports in this section.

[redacted] In the second report, the DoD OIG determined that the DoD CIO needed to improve the quality of information in the Defense Information Technology Portfolio Repository (DITPR) to permit the DoD to use the information for decision making and statutory compliance reporting.

[redacted]

[redacted]

DoD OIG Report No. DODIG-2017-082, "DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository," May 10, 2017

The DoD OIG found that DoD Components did not report complete and accurate information technology system data in the DITPR for 19 of the 31 information technology systems in its non-statistical sample. DoD guidance designates DITPR as the authoritative unclassified inventory of DoD mission critical and mission essential information technology systems.[14] Additionally, through reviews of all 6,169 information technology systems reported in DITPR as of April 20, 2016, the DoD OIG identified 2,992 information technology systems with incomplete data. For example, 11 of the 31 information technology systems in the non-statistical sample had an inaccurate number of interfacing systems. Furthermore, 1,138 information technology systems of the 6,169 information technology systems reported in DITPR did not have the Data Center Name and Location data elements completed.

As a result, the DoD cannot rely on DITPR data and has spent at least $30.8 million since 2004 to operate, maintain, and update a system that contains incomplete and inaccurate information technology system data. Unless data quality is improved, the DoD cannot effectively plan for the continued operation of mission critical and mission essential information technology systems, use DITPR for decision making as intended, or support statutory compliance reporting.

Unless data quality is improved, the DoD cannot effectively plan for the continued operation of mission critical and mission essential information technology systems, use DITPR for decision making as intended, or support statutory compliance reporting.

The DoD OIG recommended that the DoD CIO; establish a process that holds DoD Component CIOs accountable for the completeness and accuracy of information technology system data in DITPR; notify information technology system owners of data deficiencies, provide deadlines for corrections, regularly follow up with DoD Components to ensure resolution; and require training for all DITPR users and information technology system owners and add training content on DITPR purpose, statutory requirements, and relationship to DoD feeder systems.

[14] A mission critical system is a system whose loss would stop warfighter operations or direct mission support of warfighter operations. A mission essential system is a system that is basic and necessary to accomplish an organization's mission.

DoD CIO representatives agreed with the recommendations to establish an accountability process for completeness and accuracy of information system data and to notify system owners of deficiencies with deadlines and follow up. DoD CIO representatives partially agreed with the recommendation to require training and stated that they will work with stakeholders to update the current training material to incorporate increased awareness of DITPR issues.

Configuration Management

We identified nine reports with 45 recommendations addressing configuration management. Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems. Configuration management includes control of processes for initializing, changing, and monitoring the configurations of those products and systems.

~~(FOUO)~~ The following two reports are examples of how cybersecurity weaknesses in configuration management affect DoD operations. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Identity and Access Management

We identified 10 reports with 27 recommendations addressing identity and access management. Identity and access management includes the processes, technologies, and policies for managing digital identities and controlling how identities can be used to access resources.

~~(FOUO)~~ The following two reports are examples of how cybersecurity weaknesses in identity and access management affect DoD operations. Specifically, in the first report, the AFAA determined that the Air Force needed to strengthen controls over common access card (CAC) issuance and accountability for contractors. In the second report, [redacted]

AFAA Report No. F2016-0006-O40000, "Contractor Access Controls," September 26, 2016

The AFAA found that Trusted Agents did not effectively manage CAC issuance and accountability for 454 of 688 contractors reviewed, which inappropriately allowed installation and network access.[15] CACs are identification media issued to eligible contractor personnel to access DoD computer networks and installations. Before approving an application for a CAC, DoD guidance requires Trusted Agents to verify a valid need for installation and network access, verify the favorable completion of a Federal Bureau of Investigation fingerprint check, and verify the initiation of a background check. After initial CAC approval, Trusted Agents must re-verify every 6 months that a contractor has a valid, continued need for access. Finally, Air Force guidance requires Trusted Agents to collect returned CACs. The AFAA found that Trusted Agents did not retain documents to show that 218 of 400 contractors had a valid need for access, had background checks, and had provided accurate personal information. In addition, there was no evidence that Trusted Agents performed a 6-month review on any of the contractors in question. Furthermore, Trusted Agents did not retain evidence to show coordination with contracting officials prior to issuing a CAC. Instead, Trusted Agents relied on a contractor company representative to verify need for a CAC. Furthermore, of 182 contractors with justification documents, 21 were not properly vetted before receiving a CAC. For example, a contract employee was issued a CAC in June 2014, but the verification of a valid need for access did not occur until July 2015, 12 months past the requirement date. In addition, Trusted Agents did not track or retain records of returned CACs for 215 of 288 contractors. As a result, management could not determine whether CACs were sent to the nearest facility for deactivation. Finally, CACs for 37 contractors were not revoked following their employment termination date.

The AFAA found that Trusted Agents did not retain documents to show that 218 of 400 contractors had a valid need for access, had background checks, and had provided accurate personal information. In addition, there was no evidence that Trusted Agents performed a 6-month review on any of the contractors in question.

The AFAA determined that CAC issuance and accountability was not effectively managed because personnel did not comply with existing DoD or Air Force guidance for CAC issuance and accountability. In addition, the Air Force had inadequate internal control processes to ensure compliance with DoD and Air Force

[15] Trusted Agents approve contractor applications for CACs and must be U.S. citizens and a DoD uniformed service member or a DoD civilian.

guidance. Implementing effective controls over CAC issuance and accountability reduces the risk of unauthorized access to installations, resources, and sensitive information.

Implementing effective controls over CAC issuance and accountability reduces the risk of unauthorized access to installations, resources, and sensitive information.

The AFAA recommended that the Deputy Chief of Staff, Manpower, Personnel, and Services, should direct the Commander, Air Force Personnel Center to; require Trusted Agents to revoke CACs for contractors identified as no longer employed; validate the need for contractor CACs, revoke and collect unauthorized CACs; and establish Air Force Inspection System controls to ensure installation commanders comply with existing guidance over contractor CAC issuance and accountability.

The Deputy Chief of Staff, Manpower, Personnel, and Services agreed with the recommendations and cited the development of policies, procedures, and internal controls as well as updates to the Air Force Inspection System.

[redacted]

[redacted]

[redacted]

Security Training

We identified three reports with six recommendations addressing security training. Security training refers to formal activities, products, and services intended to create or enhance an individual's security knowledge or skills.

The following two reports are examples of how cybersecurity weaknesses in security training affect DoD operations. Specifically, in the first report, AFAA determined that personnel for two medical systems needed to improve the security awareness program by implementing Federal standards for system controls contained in updated DoD guidance. In the second report, the DoD OIG determined that the Defense Finance and Accounting Service (DFAS) needed to develop a formal information assurance training policy for the Defense Cash Accountability System.

AFAA Report No. F2016-0004-O10000, "Medical Systems – General and Application Controls," September 9, 2016

The AFAA found that Composite Health Care System and Defense Medical Logistics Standard Support management personnel did not monitor the security awareness program at 3 of 11 locations. The AFAA determined that the conditions occurred because Composite Health Care System and Defense Medical Logistics Standard Support personnel did not implement the NIST Risk Management Framework. Furthermore, personnel did not categorize system risk, select and implement appropriate controls, or assess those general and application controls required by NIST and the Federal Information Security Management Act. Instead, Composite Health Care System and Defense Medical Logistics Standard Support personnel followed pre-2014 DoD 8500-series policies that did not reflect current Federal regulations for general and application-specific controls. The information system control discrepancies cast doubt on the reliability of medical operations data used to administer care to beneficiaries and manage medical materiel. In addition, the Composite Health Care System and the Defense Medical Logistics Standard Support system provide information affecting Air Force financial statements. Therefore, if independent public accountants cannot rely on the system of internal controls supporting Air Force financial statements, they will have to increase substantive testing sample sizes and increase the cost of audit accordingly.

The AFAA recommended that the Air Force Surgeon General, in coordination with the Defense Health Agency and Air Force CIO, direct Composite Health Care System and Defense Medical Logistics Standard Support program managers to implement Federal NIST system control standards contained in the updated DoD Instruction 8510.01. Furthermore, the AFAA recommended that the Air Force Surgeon General establish an internal control process to validate compliance with Federal NIST system control standards contained in the updated DoD Instruction 8510.01. The Air Force Surgeon General agreed with the recommendations.

DoD OIG Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016

The DoD OIG found that the DFAS Business Enterprise Information Services Office personnel did not establish a policy to implement requirements for an information assurance training, certification, and workforce management program.[16] Although Business Enterprise Information Services personnel used an automated process to monitor when a user's information assurance training was due, the process was not formally documented in policy.

Informal policies and procedures lack the weight of authority provided by the written approval of a senior management official. The signature of a responsible authority provides clear evidence for employees and contractors that management is in agreement with the stated policies and procedures and that adherence to them is required. Without published and communicated information assurance training policy, employees may not know management's actual intent and Business Enterprise Information Services Office managers may not be able to enforce compliance.

Without published and communicated information assurance training policy, employees may not know management's actual intent and Business Enterprise Information Services Office managers may not be able to enforce compliance.

The DoD OIG recommended that the Director, Business Enterprise Information Services and Other Systems, DFAS, develop a formal information assurance training policy for Defense Cash Accountability System users.[17] The policy should include training requirements for all Defense Cash Accountability System users,

[16] Business Enterprise Information Services Office personnel are to maintain and monitor the security posture of the Defense Cash Accountability System.

[17] DoD uses the Defense Cash Accountability System to process and report its disbursement and collections of funds between the U.S. Treasury and DoD.

assign monitoring responsibilities, and inform employees of the consequences of not complying with the policy. Once formalized, they should disseminate the information assurance policies and procedures to all Defense Cash Accountability System users. The Director, Information and Technology, DFAS, agreed with the recommendation and stated that the updated Defense Cash Accountability System Access Control Policy reflects information assurance training requirements. However, the DoD OIG responded that the comments were partially responsive because they did not address monitoring responsibilities or consequences for noncompliance with training requirements. The DoD OIG requested additional comments on monitoring and consequences for noncompliance.

Information Security Continuous Monitoring

We identified four reports with nine recommendations addressing information security continuous monitoring. Information security continuous monitoring refers to maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

~~(FOUO)~~ The following two reports are examples of how cybersecurity weaknesses in information security continuous monitoring affect DoD operations. Specifically, in the first report, [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

Incident Response

We identified four reports with four recommendations addressing incident response. Incident response is the mitigation of violations of security policies and recommended practices also referred to as incident handling.

The following two reports are examples of how cybersecurity weaknesses in incident response affect DoD operations. Specifically, in the first report, GAO determined that DoD needed to define the role of the senior information security officer to ensure DoD has procedures for incident detection, response, and reporting. In the second report, GAO determined that DoD needed to improve visibility over National Guard cyber incident support capabilities and needed to conduct an exercise to prepare for a cyber incident.

GAO Report No. GAO-16-686, "Federal Chief Information Security: Opportunities Exist to Improve Roles and Address Challenges to Authority," August 26, 2016

For 3 of the 11 activities evaluated, the GAO found that the DoD did not, in accordance with Federal law and guidance, define the roles of its senior information security officer. For example, the DoD did not document in its policies the senior information security officer responsibilities for detecting, reporting, and responding to security incidents. The DoD assigned responsibility for incident response to the USCYBERCOM. Although the DoD senior information security officer said their organization is involved in USCYBERCOM incident response activities, those responsibilities and activities were not documented in DoD security policies.

GAO determined that by defining the roles of the senior information security officer, the DoD would have greater assurance that the senior information security officer is able to effectively reduce risks to DoD information and information systems and ensure agency information and information systems are adequately protected from cyber-attacks. The GAO recommended that the Secretary of Defense define the senior information security officer role in DoD policy to ensure that the DoD has procedures for incident detection, response, and reporting. The Principal Deputy DoD CIO partially agreed with the recommendation and cited USCYBERCOM responsibility for the incident handling program while acknowledging

GAO determined that by defining the roles of the senior information security officer, the DoD would have greater assurance that the senior information security officer is able to effectively reduce risks to DoD information and information systems and ensure agency information and information systems are adequately protected from cyber-attacks.

plans to publish a new incident handling manual. The GAO noted that it was important for the new manual to define clearly the role of the senior information security officer in the incident handling process. Therefore, the GAO maintained that their recommendation was still warranted.

GAO Report No. GAO-16-574, "Defense Civil Support: DoD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises," September 6, 2016

The GAO found that U.S. National Guard units had developed capabilities that could be used, if requested and approved, to support civil authorities in a cyber-incident.[18] Those capabilities include communications directorates that maintain and operate the National Guard information network, computer network defense teams that protect National Guard information systems, and cyber units that conduct cyberspace operations. However, the DoD did not have full visibility into National Guard cyber capabilities that could support civil authorities in a cyber-incident.

The DoD has conducted or participated in exercises to support civil authorities in a cyber-incident or to test the responses to simulated attacks on cyber infrastructure owned by civil authorities, but has experienced several challenges that DoD has not addressed. Those challenges include limited participant access due to a classified exercise environment, limited inclusion of other Federal agencies and critical infrastructure owners, and inadequate incorporation of joint physical-cyber scenarios. Furthermore, the DoD has not conducted a tier one exercise, which is an exercise involving national level organizations, and combatant commanders and staff, in highly complex environments.

The GAO determined that the DoD did not have visibility of all National Guard unit cyber capabilities because the DoD does not have a database that identifies cyber-related unit emergency response capabilities, as required by law. Without such a database to fully and quickly identify National Guard cyber capabilities, the DoD may not have timely access to these capabilities if and when civil authorities request them during a cyber-incident. Moreover, the DoD has not conducted a tier one exercise to prepare DoD forces to support civil authorities in a cyber-incident because DoD has not identified an exercise to do so. Conducting a tier one exercise would provide an opportunity for the DoD to address the challenges experienced

[18] Civil authorities are the elected and appointed officers and employees constituting the government at the U.S. federal, state, and territorial levels and their associated political subdivisions.

in previous exercises. Furthermore, a tier one exercise would permit the DoD to fully test response plans; evaluate response capabilities; and improve proficiency in supporting other Federal agencies, State and local authorities, if directed, in an emergency.

Furthermore, a tier one exercise would permit the DoD to fully test response plans; evaluate response capabilities; and improve proficiency in supporting other Federal agencies, State and local authorities, if directed, in an emergency.

The GAO recommended that the Secretary of Defense maintain a database that can fully and quickly identify the cyber capabilities of the National Guard in all 50 states and U.S. territories, to include the District of Columbia. The database could also be used, if requested and approved, to support civil authorities in a cyber-incident. The DoD agreed with the recommendation. Furthermore, the GAO recommended that the Secretary of Defense direct the Deputy Assistant Secretary of Defense for Cyber Policy; the Chief, National Guard Bureau; the Commander, Northern Command; and the Commander, USCYBERCOM, to conduct a tier one exercise that will improve DoD planning efforts to support civil authorities in a cyber-incident. GAO stated that such an exercise should also address challenges from prior exercises, such as limited participant access to exercise environment; inclusion of other Federal agencies and private sector cybersecurity vendors; and incorporation of emergency or disaster scenarios concurrent to cyber incidents. The Deputy Assistant Secretary of Defense, Cyber Policy, partially agreed with the recommendation, citing the Cyber Guard exercise as meeting the intent of the recommendation.[19] The GAO noted that the Cyber Guard exercise did not address the challenges from previous exercises. However, the GAO agreed that if the DoD could modify the Cyber Guard exercise to address the challenges previously cited, such as limited participant access to the exercise environment, then the exercise could improve DoD planning efforts. If the Cyber Guard exercise is not modified, the GAO maintains that the DoD should conduct a tier one exercise that includes a DoD response to support civil authorities during a cyber-incident.

Contingency Planning

We identified four reports with five recommendations addressing contingency planning. Contingency planning includes measures, such as relocation of information systems and operations to alternate sites, use of alternate equipment, or use of manual methods, to recover information system services after disruption.

[19] USCYBERCOM conducted Cyber Guard exercises in FYs 2013 – 2015 to explore the ability of the DoD, other Federal agencies, and the private sector to respond in cyberspace to a destructive or disruptive attack of significant consequence on U.S. critical infrastructure.

The following two reports are examples of how cybersecurity weaknesses in contingency planning affect DoD operations. Specifically, in the first report, the DoD OIG determined that DFAS needed to develop processes to incorporate lessons learned from after action reports into the Defense Cash Accountability System contingency plan. In the second report, the AFAA determined that personnel for two medical systems needed to improve contingency planning controls by implementing Federal standards for system controls contained in updated DoD guidance.

DoD OIG Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016

The DoD OIG found that DFAS Business Enterprise Information Services Office personnel did not update or revise the Defense Cash Accountability System contingency plan to correct deficiencies identified during testing of the plan. NIST requires that the plan coordinator update the contingency plan, if appropriate, by implementing recommendations made because of testing. Contingency test results provide an important measure of the plan's feasibility. Any testing of the plan is likely to identify weaknesses, and it is important that the plan and related supporting activities be revised to address these weaknesses.

The DoD OIG recommended that the Director of Business Enterprise Information Services and Other Systems, DFAS, develop and implement processes to incorporate lessons learned from the contingency plan after action report into the Defense Cash Accountability System contingency plan in a timely manner. The Director, Information and Technology, DFAS, agreed with the recommendation citing two after action reports that had been issued in a timely manner and had incorporated lessons learned from the contingency plan. The DoD OIG requested additional comments that specifically addressed the incorporation of lessons learned from the contingency plan after action report into the contingency plan for the Defense Cash Accountability System.

AFAA Report No. F2016-0004-O10000, "Medical Systems – General and Application Controls," September 9, 2016

The AFAA found that Composite Health Care System and Defense Medical Logistics Standard Support management personnel did not implement required contingency planning controls. Specifically, management personnel did not properly assess the criticality and sensitivity of computerized operations. Likewise, they did not identify supporting resources or complete the required business impact analysis to pinpoint critical information technology resources, disruption impacts, allowed outage times, and recovery priorities at 9 of 11 locations. In addition, management personnel did not take adequate steps to prevent and minimize potential damage and system interruption or develop, document, or test comprehensive contingency plans.

Management personnel did not take adequate steps to prevent and minimize potential damage and system interruption or develop, document, or test comprehensive contingency plans.

The AFAA determined that the conditions occurred because Composite Health Care System and Defense Medical Logistics Standard Support personnel did not implement the NIST Risk Management Framework. Furthermore, personnel did not categorize system risk, select and implement appropriate controls, or assess those general and application controls required by NIST and the Federal Information Security Management Act. Instead, Composite Health Care System and Defense Medical Logistics Standard Support personnel followed pre-2014 DoD 8500-series policies that did not reflect current Federal regulations for general and application controls. The discrepancies found in the information system controls cast doubt on the reliability of medical operations data used to administer care to beneficiaries and manage medical materiel. In addition, the Composite Health Care System and the Defense Medical Logistics Standard Support system provide information affecting the Air Force financial statements. Therefore, if independent public accountants cannot rely on the system of internal controls supporting Air Force financial statements, they will have to increase sample sizes for substantive testing and increase the cost of audit accordingly.

The AFAA recommended that the Air Force Surgeon General, in coordination with the Defense Health Agency and Air Force CIO, direct Composite Health Care System and Defense Medical Logistics Standard Support program management personnel to implement Federal NIST system control standards contained in the updated DoD Instruction 8510.01. Furthermore, the AFAA recommended that the Air Force Surgeon General establish an internal control process to validate compliance with Federal NIST system control standards contained in the updated DoD Instruction 8510.01. The Air Force Surgeon General agreed with the recommendations.

Summary

We prepared Section II to summarize the reports in alignment with the FY 2017 IG FISMA Reporting Metrics to support the preparation of our annual FISMA evaluation. The 26 reports in this section are a subset of the 29 reports from Section I and, thus the most pervasive DoD cybersecurity weaknesses are discussed in the Summary for Section I. This occurred because the FY 2017 IG FISMA Reporting Metrics do not always directly align with the NIST Cybersecurity

Framework functions outlined in Table 2 of the Introduction. For example, the preparation and testing of contingency plans is part of the Contingency Planning metric in the FY 2017 IG FISMA Reporting Metrics, but is part of the Protect function versus the Recover function in the NIST Cybersecurity Framework. The execution of a plan is part of the Recover function. This explains how the oversight community could cover the Contingency Planning metric under FISMA, but not cover the Recover function under the NIST Cybersecurity Framework. See the summary for Section I for a more comprehensive discussion of the most pervasive DoD cybersecurity weaknesses.

Appendix A

Scope and Methodology

We conducted this summary work from April 2017 through June 2018. We followed generally accepted government auditing standards, except for the standards of planning and evidence because the report summarizes previously released reports. This summary report supports the DoD OIG response to the requirements of Public Law 106-531, "Reports Consolidation Act of 2000," section 3516(d), November 22, 2000, and Public Law Public Law 113 283, "Federal Information Security Modernization Act of 2014," section 3555, December 18, 2014.

This report summarizes the DoD cybersecurity weaknesses identified in 29 unclassified reports and 1 testimony, which were issued by the DoD oversight community and GAO from July 1, 2016, through June 30, 2017. Specifically, we summarized the DoD cybersecurity weaknesses using the NIST Cybersecurity Framework and the FY 2017 IG FISMA Reporting Metrics. Furthermore, we extended our initial objective from the DoD audit community to include the DoD oversight community, as represented by the members of the Defense Council on Integrity and Efficiency Information Technology Committee. We coordinated with the DoD oversight community and the GAO to obtain the unclassified reports and testimonies in this summary. We did not review the supporting documentation for any of the reports. Because the issued reports contained recommendations related to the identified cybersecurity weaknesses, we did not make any new or additional recommendations in this report.

Use of Computer-Processed Data

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

Prior Coverage

During the last 6 years, the DoD OIG issued five reports summarizing cybersecurity weaknesses identified in 129 audit reports and testimonies issued by the DoD 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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Appendix B

Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017

GAO

Report No. GAO-17-369, "Department of Defense: Actions Needed to Address Five Key Mission Challenges," June 13, 2017

[redacted]

Report No. GAO-17-322, "DoD Major Automated Information Systems: Improvements Can Be Made in Applying Leading Practices for Managing Risk and Testing," March 30, 2017

Testimony No. GAO-17-263T, "Information Technology: Improved Implementation of Reform Law Is Critical to Better Manage Acquisitions and Operations," December 6, 2016

Report No. GAO-17-8, "IT Workforce: Key Practices Help Ensure Strong Integrated Program Teams; Selected Departments Need to Assess Skill Gaps," November 30, 2016

Report No. GAO-16-511, "Information Technology: Agencies Need to Improve Their Application Inventories to Achieve Additional Savings," September 29, 2016

Report No. GAO-16-574, "Defense Civil Support: DoD Needs to Identify National Guard's Cyber Capabilities and Address Challenges in Its Exercises," September 6, 2016

Report No. GAO-16-686, "Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority," August 26, 2016

Report No. GAO-16-469, "Information Technology Reform: Agencies Need to Increase Their Use of Incremental Development Practices," August 16, 2016

Report No. GAO-16-593, "Joint Information Environment: DoD Needs to Strengthen Governance and Management," July 14, 2016

DoD OIG

Report No. DODIG-2017-082, "DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository," May 10, 2017

[redacted]

Report No. DODIG-2017-068, "Strategic Plan Needed for Navy Financial Management Systems," March 16, 2017

[redacted]

Report No. DODIG-2017-015, "Application Level General Controls for the Defense Cash Accountability System Need Improvement," November 10, 2016

[redacted]

Army Inspector General

[redacted]

[redacted]

Army Audit Agency

[redacted]

[redacted]

[redacted]

Air Force Audit Agency

Report No. F2017-0004-O10000, "Risk Management Framework Implementation – Financial Systems," May 15, 2017

Report No. F2017-0002-L20000, "Electronic Pod Management," January 5, 2017

Report No. F2017-0002-L10000, "Air Force General Fund and Working Capital Fund General Equipment – Information Technology Hardware Existence and Completeness," January 5, 2017

[redacted]

Report No. F2016-0006-O40000, "Contractor Access Controls," September 26, 2016

Report No. F2016-0006-O10000, "Air Forces Central Command Morale Network Operation," September 9, 2016

Report No. F2016-0005-O10000, "Air Forces Central Command Wireless Network Security," September 9, 2016

Report No. F2016-0004-O10000, "Medical Systems – General and Application Controls," September 9, 2016

[redacted]

Appendix C

Matrix of Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017, by NIST Cybersecurity Framework Identify Function Category

Agency Report No.	NIST Cybersecurity Framework Identify Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy
Government Accountability Office					
GAO-17-369	X	X	X	X	
[redacted]			X	X	
GAO-17-322	X	X			X
GAO-17-263T	X		X		
GAO-17-8	X				
GAO-16-511	X				
GAO-16-574	X				
GAO-16-686	X		X		
GAO-16-469	X		X		
GAO-16-593		X	X		X
DoD Inspector General					
DODIG-2017-082	X				
[redacted]			X		
[redacted]	X				
DODIG-2017-015	X		X		
[redacted]	X				
Army Inspector General					
[redacted]	X		X	X	
[redacted]	X		X		
Army Audit Agency					
[redacted]				X	

Matrix of Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017, by NIST Cybersecurity Framework Identify Function Category (cont'd)

Agency Report No.	NIST Cybersecurity Framework Identify Function Category				
	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy
Air Force Audit Agency					
F2017-0004-O10000	X				X
F2017-0002-L20000	X				
F2017-0002-L10000	X				
[redacted]					X
F2016-0006-O10000	X				
F2016-0005-O10000	X				
F2016-0004-O10000	X			X	
[redacted]	X				

Source: The DoD OIG.

Appendix D

Matrix of Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017, by NIST Cybersecurity Framework Protect Function Category

Agency Report No.	NIST Cybersecurity Framework Protect Function Category					
	Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology
Government Accountability Office						
GAO-17-369				X		
[redacted]				X		
GAO-17-322				X		
GAO-16-574				X		
DoD Inspector General						
[redacted]				X		
DODIG-2017-068						X
[redacted]	X		X	X		X
DODIG-2017-015	X	X		X		
[redacted]	X					
Army Inspector General						
[redacted]		X		X		
[redacted]				X	X	
Army Audit Agency						
[redacted]				X		
[redacted]	X					

Matrix of Reports Issued and Testimonies From July 1, 2016, Through June 30, 2017, by NIST Cybersecurity Framework Protect Function Category (cont'd)

Agency Report No.	NIST Cybersecurity Framework Protect Function Category					
	Access Control	Awareness & Training	Data Security	Information Protection Processes & Procedures	Maintenance	Protective Technology
Air Force Audit Agency						
F-2016-0004-O10000	X	X		X		X
F-2016-0005-O10000	X					
F-2016-0006-O10000	X					X
F-2016-0006-O40000	X					
F-2017-0002-L20000	X					

Source: The DoD OIG.

Appendix E

Matrix of Reports Issued From July 1, 2016, Through June 30, 2017, by FY 2017 IG FISMA Reporting Metric

Agency Report No.	FY 2017 IG FISMA Reporting Metrics						
	Risk Management	Configuration Management	Identity and Access Management	Security Training	Information Security Continuous Monitoring	Incident Response	Contingency Planning
Government Accountability Office							
GAO-17-369	X					X	X
[redacted]	X	X	X		X		
GAO-17-322	X	X					
GAO-16-574	X					X	
GAO-16-686	X					X	
GAO-16-593	X						
DoD Inspector General							
DODIG-2017-082	X						
[redacted]	X				X		X
DODIG-2017-068		X					
[redacted]	X	X	X				
DODIG-2017-015	X	X	X	X			X
[redacted]	X		X				
Army Inspector General							
[redacted]	X	X		X	X		
[redacted]	X	X					

Matrix of Reports Issued From July 1, 2016, Through June 30, 2017, by FY 2017 IG FISMA Reporting Metric (cont'd)

Agency Report No.	FY 2017 IG FISMA Reporting Metrics						
	Risk Management	Configuration Management	Identity and Access Management	Security Training	Information Security Continuous Monitoring	Incident Response	Contingency Planning
Army Audit Agency							
[redacted]		X					
[redacted]					X		
[redacted]			X				
Air Force Audit Agency							
F2017-0004-O10000	X						
F2017-0002-L20000	X		X				
F2017-0002-L10000	X						
[redacted]	X						
F2016-0006-O40000			X				
F2016-0006-O10000	X		X				
F2016-0005-O10000	X		X				
F2016-0004-O10000	X	X	X	X		X	X
[redacted]	X						

Source: The DoD OIG.

Acronyms and Abbreviations

AAA	Army Audit Agency
AFAA	Air Force Audit Agency
AFCENT	Air Forces Central Command
CAC	Common Access Card
CIO	Chief Information Officer
DCIE	Defense Council on Integrity and Efficiency
DFAS	Defense Finance and Accounting Service
DITPR	DoD Information Technology Portfolio Repository
FISMA	Federal Information Security Modernization Act
GAO	Government Accountability Office
NIST	National Institute of Standards and Technology
USCYBERCOM	U.S. Cyber Command

Whistleblower Protection

U.S. Department of Defense

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/.

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