Report No. DODIG-2019-089

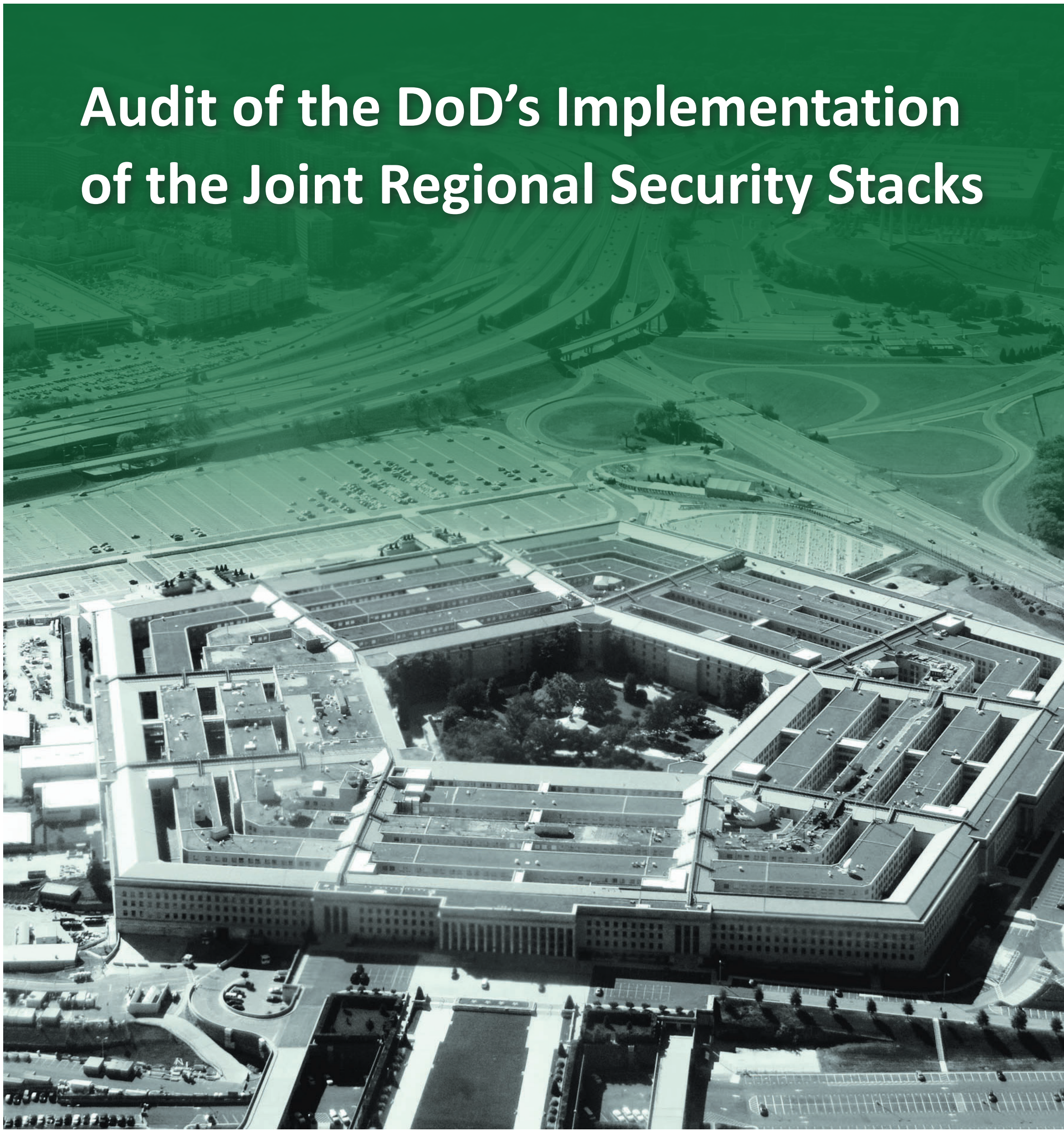
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

JUNE 4, 2019

Audit of the DoD's Implementation of the Joint Regional Security Stacks



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

Audit of the DoD's Implementation of the Joint Regional Security Stacks

June 4, 2019

Objective

We determined whether the DoD's implementation of the Joint Regional Security Stacks (JRSS) is achieving the expected outcomes of the DoD's Joint Information Environment (JIE) objective to implement regional security. The expected outcomes of implementing regional security are to:

- provide timely access to trusted cyber situational awareness that will provide the DoD an understanding of its security posture and threat environment, related risk, and the entity's projected future status;
- reduce the number of paths an adversary can use to gain access to the DoD Information Network (DoDIN); and
- improve the DoDIN security posture.[1]

Background

In August 2010, the Secretary of Defense initiated the JIE to consolidate the DoD's information technology infrastructure into a single security architecture that is intended to improve the DoD's ability to defend its network against cyber attacks. The DoD Chief Information Officer (CIO) proposed to the JIE Executive Committee that the DoD should implement the JRSS to address the JIE capability objective of implementing regional security.

Background (cont'd)

The JRSS is a suite of equipment that includes assets such as network routers, firewalls, and switches that work together to:

- provide network security capabilities, such as intrusion detection and prevention;
- reduce the number of access points to the DoDIN;
- enable inspections of network traffic that travels through the JRSS;
- serve as the network traffic flow integration point between DoD Components; and
- facilitate the monitoring and control of all security mechanisms throughout the DoD network.

Finding

The DoD's implementation of the JRSS is not fully achieving the expected outcomes of the DoD's JIE objective to implement regional security. Although implementing the JRSS is reducing the footprint and number of enemy attack vectors to the DoDIN, the JRSS is not achieving other intended JIE outcomes for implementing regional security. Specifically:

- ~~(U//FOUO)~~ [redacted] and
- ~~(U//FOUO)~~ [redacted]

The JRSS is not meeting other JIE outcomes because DoD officials did not ensure that all JRSS tools met users' needs and that JRSS operators were trained prior to JRSS deployment. In addition, although the JRSS was estimated to cost over $520 million, DoD officials considered the JRSS to be a technology refresh and, therefore, not

[1] Security posture is the status of an entity's networks based on the people, hardware, software, policies, and capabilities in place to protect and defend its information and information systems.

Visit us at www.dodig.mil

Results in Brief

Audit of the DoD's Implementation of the Joint Regional Security Stacks

Finding (cont'd)

subject to DoD Instruction 5000.02 requirements.[2] Had DoD Instruction 5000.02 requirements applied, the JRSS would have qualified as a major automated information system acquisition because it is projected to cost $1.7 billion more than the $520 million threshold and DoD officials would have been required to develop formal capability requirements, an approved test and evaluation master plan, and a training plan for operators during the development of the JRSS.

~~(U//FOUO)~~ The Defense Information Systems Agency (DISA) serves as the JRSS program management office and is responsible for identifying and successfully remediating vulnerabilities and developing plans of action and milestones for vulnerabilities that cannot be remediated. [redacted][3] This occurred because the JRSS Program Management Officer did not ensure that DISA officials managed vulnerabilities in accordance with the JRSS Vulnerability Management Plan.

According to the Director of DoDIN Modernization, the JRSS is the most critical near-term element of the DoD's JIE. Therefore, if the JRSS is not operationally effective, secure, and sustainable, the DoD may not achieve the JIE vision, which includes achieving greater security on the DoDIN. In addition, without adequate security safeguards for the JRSS, weaknesses identified in this report could prevent network defenders from obtaining the information necessary to make timely decisions, and could lead to unauthorized access to the DoDIN and the destruction, manipulation, or compromise of DoD data.

Management Actions Taken

~~(U//FOUO)~~ In December 2018, the DoD CIO issued a memorandum describing actions that the DoD CIO plans to take to improve JRSS operations. The DoD CIO issued the memorandum in response to recommendations made by the Director of Operational Test and Evaluation in a December 2018 annual report. Although the DoD CIO's memorandum addressed training challenges identified in this report, it did not specify whether the DoD CIO plans to develop and implement a schedule for providing all JRSS operators with JRSS scenario-based training and lab-based exercises. Therefore, we are making a recommendation to the DISA Director, who is responsible for providing training and technical support and overseeing network and security services, to develop and implement a schedule to ensure that all JRSS operators receive the training needed to use the JRSS as intended. In addition, during our audit, we informed the JRSS program management office that some capabilities were not meeting users' needs. [redacted]

Recommendations

We recommend that the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the DoD CIO, establish or revise guidance that requires DoD Components to follow the same requirements when developing a technology refresh that will exceed an established cost threshold as required for new acquisitions under DoD Instruction 5000.02.

[2] DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, (Incorporating Change 3, August 10, 2017). A technology refresh is an incremental insertion of newer technology to improve reliability, improve maintainability, reduce cost, and add minor performance enhancements.

[3] Critical and high vulnerabilities are vulnerabilities that would allow adversaries to directly and immediately compromise the confidentiality, integrity, or availability of systems and data.

Results in Brief

Audit of the DoD's Implementation of the Joint Regional Security Stacks

Recommendations (cont'd)

We also recommend that the DoD CIO, in coordination with the DISA Director, develop a baseline JRSS functional capabilities requirement document that includes all capabilities required for the JRSS to meet user needs and the expected outcomes of implementing regional security.

We recommend that the DISA Director direct the JRSS Program Management Officer to:

- establish and implement a plan to incorporate the required capabilities into the JRSS once the JRSS functional capabilities requirement document is developed;
- develop and implement a schedule to provide all JRSS operators with training, as required by the JRSS Operations Training Requirements Document; and
- ~~(U//FOUO)~~ [redacted]

Management Comments and Our Response

The Assistant Secretary of Defense for Acquisition, responding for the Under Secretary of Defense for Acquisition and Sustainment, agreed with the intent of our recommendation to rigorously manage technology refresh programs, but not to establish a fixed threshold that would require all such programs to be managed as "new programs." The Assistant Secretary stated that the Office of the Under Secretary of Defense for Acquisition and Sustainment is developing policy for unique characteristics of information systems and commercial off-the-shelf hardware and will consider the intent of the recommendation in that context. However, the Assistant Secretary did not explain how the new guidance will address the processes and procedures that should be followed when acquiring technology refreshes; therefore, the recommendation is unresolved. We request additional comments from the Under Secretary of Defense explaining how the new guidance will address processes and procedures that must be followed when acquiring technology refreshes.

The Principal Deputy CIO, responding for the DoD CIO, disagreed with the recommendation to develop a baseline functional capabilities requirement document, stating that the DoD developed a functional requirements document that was coordinated with all stakeholders and approved by the DoD CIO. The Principle Deputy stated that they will review and if required, update the JRSS measures of effectiveness and measures of performance; map the JRSS capability requirements to the corresponding measures of effectiveness and measures of performance; and add an appendix to the functional requirements document to include the measures of effectiveness and measures of performance. Although the Principle Deputy disagreed, the proposed actions addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we verify the agreed upon actions are implemented.

The DISA Director agreed with the recommendations stating that DISA will:

- propose a plan to address changes identified during testing after the measures of performance assessment;
- work with DoD Officials to incorporate JRSS operational training requirements into the Components' institutional training programs; and

Management Comments (cont'd)

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

The DISA Director addressed all specifics of the recommendations; therefore, the recommendations are resolved. We will close the recommendations once we verify that the agreed upon actions are implemented.

Please see the Recommendations Table on the next page for the status of the recommendations.

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Under Secretary of Defense for Acquisition and Sustainment	1	None	None
DoD Chief Information Officer	None	2	None
Director, Defense Information Systems Agency	None	3.a, 3.b, 3.c	None

Please provide Management Comments by July 5, 2019.

Note: The following categories are used to describe agency management's comments to individual recommendations.

- **Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **Closed** – OIG verified that the agreed upon corrective actions were implemented.

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

June 4, 2019

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION
AND SUSTAINMENT
COMMANDER, U.S. CYBER COMMAND
DOD CHIEF INFORMATION OFFICER
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
AUDITOR GENERAL, DEPARTMENT OF THE ARMY
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: Audit of the DoD's Implementation of the Joint Regional Security Stacks
(Report No. DODIG-2019-089)

We are providing this report for review and comment. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments from the Office of the Under Secretary of Defense for Acquisition and Sustainment, Office of the DoD Chief Information Officer, and Defense Information Systems Agency on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Office of the Under Secretary of Defense for Acquisition and Sustainment did not address the specifics of Recommendation 1. Therefore, we request additional comments on the recommendation by July 5, 2019.

Please send a PDF file containing your comments to audcso@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the cooperation and assistance received during the audit. Please direct questions to me at (703) 699-7331 (DSN 499-7331).

Carol N. Gorman

Carol N. Gorman
Assistant Inspector General for Audit
Cyberspace Operations

Contents

Introduction

Finding. The DoD's Implementation of the JRSS is Not Fully Achieving the Expected JIE Outcomes ... 8

Appendix

Management Comments

Acronyms and Abbreviations ... 32

Introduction

Objective

Our objective was to determine whether the DoD's implementation of the Joint Regional Security Stacks (JRSS) is achieving the expected outcomes of the DoD's Joint Information Environment (JIE) objective to implement regional security. The expected outcomes of implementing regional security are to:

- provide timely access to trusted cyber situational awareness that will provide the DoD an understanding of its security posture and threat environment, related risk, and projected future status;
- reduce the number of paths an adversary can use to gain access to the DoD Information Network (DoDIN); and
- improve the DoDIN security posture.

See the Appendix for a discussion of the scope, methodology, and prior coverage.

Background

In August 2010, the Secretary of Defense initiated the JIE to consolidate the DoD's information technology (IT) infrastructure into a single security architecture that is intended to improve the DoD's ability to defend its network against cyber attacks. A single security architecture enables global and regional cyber situational awareness by providing DoD commanders and users with information on the availability, performance, security, and readiness of JIE services and infrastructure. The JIE contains 10 capability objectives, as described in Table 1.

Table 1. Joint Information Environment Capability Objectives

Capability Objective	Outcome of Implementation
Implement Regional Security	Timely access to trusted cyber situational awareness; reduced footprint and enemy attack vectors; improved security posture for DoD Information Network Operations and Defensive Cyber Operations–Internal Defense Measures
Modernize Network Infrastructure	Information available to enable timely decisions
Enable Enterprise Network Operations	Operation centers that secure, operate, and defend the Defense Information System Network, denying adversaries the freedom of maneuver within the DoD's cyberspace domain
Provide Mission Partner Environment-Information System	Rapid creation of Communities of Interest; enhanced coordination and command and control between combatant commands and mission partners to support operations
Optimize Data Center Infrastructure	Optimized computing infrastructure replicated across data centers for survivability and to enable timely decision making

Table 1. Joint Information Environment Capability Objectives (cont'd)

Capability Objective	Outcome of Implementation
Implement Consistent Cybersecurity Protections	Anonymity driven out of DoD networks; timely decision making enabled*
Enhance Enterprise Mobility	Seamless access to information and computing power from any location to enable timely decision making
Standardize IT Commodity Management	Streamlined software, hardware, services; hardened end points enable cross-combatant command collaboration for trans-regional threats
Establish End-User Enterprise Services	Common applications and services for joint use across DoD; standard baselines enable cross-combatant command collaboration for trans-regional threats
Provide Hybrid Cloud Computing Environments	Accelerated application migration to the Cloud for improved efficiency; supports timely decision making

* Implementing consistent cybersecurity protections uses a combination of initiatives, such as identity and access management, to allow network defenders to identify who is on DoD networks and ensure that authorized personnel conduct only approved activities on the networks.

Source: DoD Chief Information Officer (DoD CIO).

In September 2014, the DoD CIO, who is responsible for establishing policy and guidance to support DoDIN operations and defensive measures, proposed to the JIE Executive Committee that the DoD should implement the JRSS to address the JIE capability objective of implementing regional security.[4] Implementing regional security refers to using the JRSS to provide protected communications between installations and combatant command, Military Service, and DoD agency networks. According to the DoD CIO, achieving this capability objective will result in timely access to cyber situational awareness, reduced footprint and enemy attack vectors, and an improved security posture for DoDIN operations. An enterprise's security posture relies on people, hardware, software, policies, and capabilities to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.[5]

Joint Regional Security Stacks

In November 2015, the Secretary of Defense directed the DoD CIO to designate the JRSS as an enterprise service and for the DoD to migrate to the JRSS by the end of FY 2019.

[4] The JIE Executive Committee includes stakeholders from across the DoD who oversee the 10 JIE capability objectives and provide approval for capability requirements, solutions, funding, and scheduling.

[5] According to the National Institute of Standards and Technology, non-repudiation is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

The JRSS is a suite of equipment that includes assets, such as network routers, firewalls, and switches that work together to:

- provide network security capabilities, such as intrusion detection and prevention;
- reduce the number of access points to the DoD network;
- enable inspections of network traffic that travels through the JRSS;
- serve as the network traffic flow integration point between DoD Components; and
- facilitate the monitoring and control of all security mechanisms throughout the DoD network.

The JRSS also provides situational awareness by collecting data that allows operators to analyze cyber information from the DoDIN so they can troubleshoot issues occurring on the network and detect threats. For example, sensor data within the JRSS provides operators with information about suspicious network activity, such as adversaries gaining unauthorized access to the network, leading to more successful mitigation efforts and reduced impact to the mission readiness of DoD Components.

The JRSS represents a shift from protecting Service-specific networks and systems to securing the DoD enterprise in a unified manner. The JRSS centralizes the DoD's network security into regional architectures instead of local architectures at each military base, post, camp, or station. The DoD CIO plans to replace more than 1,000 local security stacks with 23 Non-Secure Internet Protocol Router Network (NIPRNET) JRSS and 25 Secret Internet Protocol Router Network JRSS at locations around the world.[6] As of March 2019, the Defense Information Systems Agency (DISA), which serves as the JRSS program management office (PMO), deployed 13 of the 23 planned NIPRNET JRSS and planned to deploy the remaining 10 by October 2019.[7] As of March 2019, none of the Secret Internet Protocol Router Network JRSS were deployed.

The NIPRNET JRSS typically consists of 20 equipment racks of security devices, which are divided into two layers—an agency layer and a base layer. The agency layer security devices operate based on Component-wide policies while the base layer security devices operate based on installation-specific policies. For example,

[6] The Non-Secure Internet Protocol Router Networks supports internet connectivity and unclassified information exchange for DoD applications, such as e-mail, web services, and file transfer, and provides the DoD with centralized and protected access to the public internet. The Secret Internet Protocol Router Network supports secret information exchange for official DoD business applications, such as e-mail, web services, and file transfer, providing access to a joint, shared DoD environment at the secret classification level for the exchange of information among the DoD components.

[7] For the purposes of this report, we define "deployed" as stacks that are receiving network traffic.

Army firewalls limit network traffic based on firewall rules set for the entire Army, while base-level firewalls at Fort Bragg, North Carolina, limit network traffic according to Fort Bragg's specific firewall rules. DoD operational traffic is routed through some or all of the security devices depending on the type of content within the data flows being processed or inspected. Figure 1 shows the JRSS used for NIPRNET.

Figure 1. Non-Secure Internet Protocol Router Network JRSS
Source: The DoD CIO.

JRSS Operators

~~(U//FOUO)~~ There are two primary types of JRSS operators—enterprise and DoD Component-specific operators. Enterprise JRSS operators are generally assigned to DISA and conduct JRSS activities in support of the Global Cyberspace Operations mission. DoD Component operators may be responsible for monitoring network activity regionally, depending on the Component's mission. [redacted]

JRSS operators use the Joint Management System (JMS) to remotely monitor the network activity that flows through the JRSS and perform defensive cyber operations, such as supporting efforts to remove adversary presence and strengthening the cyberspace environment. The JMS is a critical JRSS component that enables situational awareness for strategic, regional, and local command and control activities. According to the JRSS Implementation Plan, the JMS allows operators at the network operations center to use JRSS sensors to see through the entire network with better reliability, providing enhanced, precise, and timely information on network operations.[8] In particular, the JMS is intended to allow JRSS operators to monitor the portion of the Defense Information System Network they are responsible for protecting, including network activity at each DoD installation.

DISA officials plan to field six JMS NIPRNET hubs. As of November 2018, three were operational and the remaining three were expected to be operational by FY 2020.

JRSS Management and Support

U.S. Cyber Command, the DoD CIO, DISA, and Service cyber component officials have roles and responsibilities for JRSS management and support.

U.S. Cyber Command is responsible for developing JRSS joint operational procedures, managing the authoritative list of JRSS operational requirements, and working with DoD Components to develop JRSS joint operation training and exercises. In addition, on August 21, 2017, U.S. Cyber Command released the JRSS Concept of Operations, which is the authoritative document for global JRSS operations.[9] U.S. Cyber Command is also responsible for overseeing the DoD's vulnerability management program. In this role, U.S. Cyber Command develops and issues policy on vulnerability management.

The DoD CIO establishes policy and guidance to support DoDIN operations and defensive measures for the JRSS. In that role, the DoD CIO prepared the JRSS Implementation Plan and oversees the JRSS implementation effort.

DISA serves as the JRSS PMO. The JRSS PMO is responsible for directing the vulnerability management process, which includes identifying and successfully remediating vulnerabilities and developing plans of action and milestones for vulnerabilities that cannot be remediated. In addition, the JRSS Program Management Officer is responsible for overseeing the JRSS vulnerability management program. Furthermore, DISA ensures that JRSS equipment is operational and meets users' needs. DISA is also responsible for providing training

[8] DoD CIO Joint Regional Security Stack Implementation Plan FY16-21, version 1.2, November 3, 2015.

[9] U.S. Cyber Command Joint Regional Security Stack Concept of Operations, August 21, 2017.

and technical support and overseeing network and security services. DISA Global Operations Command operates and manages the JRSS, the JMS, and defensive cyber operations.

The Service cyber components serve as the central operational authorities for cyberspace operations and leverage the JRSS as a cyberspace defensive capability.

Guidance for Information System Acquisitions

DoD Instruction 5000.02 "provides management principles and mandatory policies and procedures for managing all acquisition programs."[10] DoD Instruction 5000.02 states that acquisitions of automated information systems that are estimated to exceed $520 million from the first phase of acquisition through sustainment are Major Automated Information Systems programs. The Instruction requires acquisition documents, such as approved capability requirements and an approved test and evaluation master plan, which help ensure that the product meets users' needs.

DoD officials considered the implementation of the JRSS to be a technology refresh to the existing Service-level security stacks.[11] The DISA IT Acquisition Guide provides guidance for the acquisition of all DISA IT products and services and is applicable to DISA acquisition programs, pilots, projects, and initiatives, which includes technology refreshes. The Guide provides customized and streamlined acquisition models that align with DoD Instruction 5000.02 to account for the diverse set of IT capabilities DISA acquires. In particular, the IT Acquisition Guide defines the standard acquisition processes that DISA should follow to acquire products or services (such as those for the JRSS) for its customers (the DoD Components). For example, the IT Acquisition Guide requires DISA to document capability and performance requirements and conduct testing to verify that programs meet performance and functional requirements. A system's performance requirements are defined in its key performance parameters. DoD Instruction 5000.02 refers to the Defense Acquisition University for a complete glossary of acquisition terms. According to the Defense Acquisition University Glossary, key performance parameters are the performance attributes of a system that are critical or essential to the development of an effective capability. These performance attributes are expressed in measureable terms, such as speed, payload, range, time-on-station, and frequency.

[10] DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, (Incorporating Change 3, August 10, 2017). DoD Instruction 5000.02 was updated on August 31, 2018, to incorporate Change 4. However, the change did not reflect information used in this report. An acquisition program is a directed, funded effort that provides a new, improved, or continuing materiel, weapon or information system, or service capability in response to an approved need.

[11] A technology refresh is an incremental insertion of newer technology to improve reliability, improve maintainability, reduce cost, and add minor performance enhancements.

Review of Internal Controls

DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.[12] We identified internal control weaknesses in the DoD's implementation of the JRSS, including a lack of requirements management, vulnerability remediation, and operator training. We will provide a copy of the report to the senior officials responsible for internal controls.

[12] DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

The DoD's Implementation of the JRSS is Not Fully Achieving the Expected JIE Outcomes

The DoD's implementation of the JRSS is not fully achieving the expected outcomes of the DoD's JIE objective to implement regional security. Although implementing the JRSS is reducing the footprint and number of enemy attack vectors to the DoDIN, the JRSS is not achieving other intended JIE outcomes for implementing regional security. Specifically:

- ~~(U//FOUO)~~ [redacted] and
- ~~(U//FOUO)~~ [redacted]

The JRSS is not meeting the other JIE outcomes because DoD officials did not ensure that all JRSS tools met users' needs and that JRSS operators were trained prior to JRSS deployment. In addition, although the JRSS was estimated to cost over $520 million, DoD officials considered the JRSS to be a technology refresh and, therefore, not subject to DoD Instruction 5000.02 requirements. Had DoD Instruction 5000.02 requirements been applied, the JRSS would qualify as a major automated information system acquisition because it is projected to cost $1.7 billion more than the $520 million threshold, and DoD officials would have been required to develop formal capability requirements, an approved test and evaluation master plan, and a training plan for operators during the development of the JRSS.

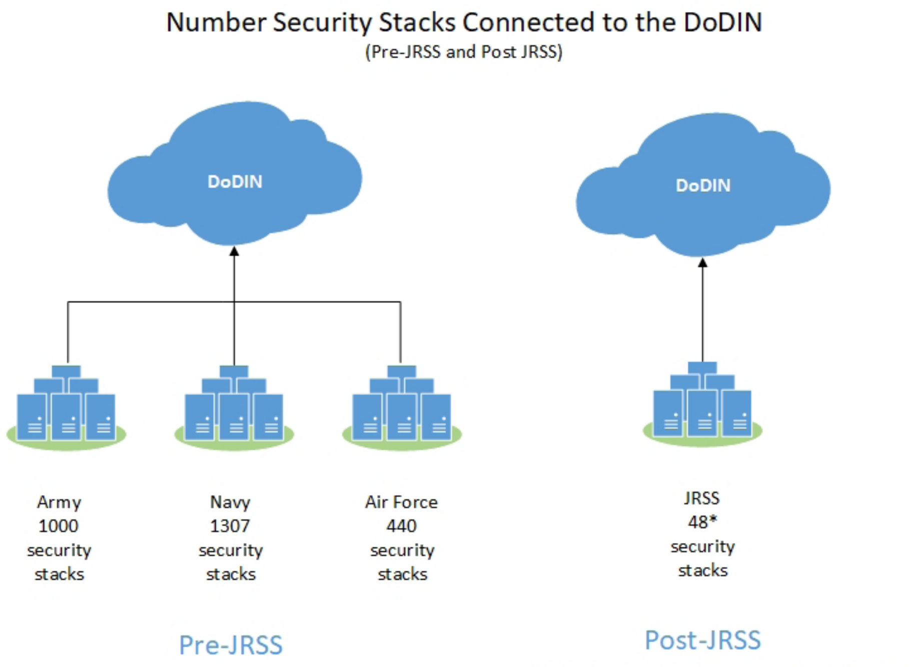
~~(U//FOUO)~~ DISA serves as the JRSS PMO and is responsible for identifying and successfully remediating vulnerabilities and developing plans of action and milestones for vulnerabilities that cannot be remediated. [redacted] This occurred because the JRSS Program Management Officer did not ensure that DISA officials managed vulnerabilities in accordance with the JRSS Vulnerability Management Plan.

According to the Director of DoDIN Modernization, the JRSS is the most critical near-term element of the DoD's JIE. Therefore, if the JRSS is not operationally effective, secure, and sustainable, the DoD may not achieve the JIE vision, which includes achieving greater security on the DoDIN. In addition, without adequate security safeguards for the JRSS, weaknesses identified in this report could prevent network defenders from obtaining the information necessary to make timely decisions, and could lead to unauthorized access to the DoDIN and the destruction, manipulation, or compromise of DoD data.

JRSS Implementation Is Reducing the Number of Attack Vectors to the DoD Information Network

Implementing the JRSS is reducing the number of enemy attack vectors to the DoDIN. When the JRSS is deployed, DoD Components use it to gain access to the DoDIN and discontinue use of their individual security stacks. Since each security stack contains at least one access point to the DoDIN, reducing the number of security stacks reduces the number of access points, thus providing fewer opportunities for an adversary to access the DoDIN. Figure 2 shows the number of access points to the DoDIN before and after the planned JRSS implementation is complete.

Figure 2. Reduction of the Number of Access Points to the DoDIN (Pre-JRSS and Post-JRSS)



**Note: The target architecture for the JRSS is 48 JRSS security stacks (23 NIPRNET and 25 SIPRNET).*

Source: The DoD OIG.

As of March 2019, DISA officials deployed 13 of the 23 planned NIPRNET JRSS around the world, reducing the number of individual access points by 131.[13]

As of March 2019, DISA officials deployed 13 of the 23 planned NIPRNET JRSS around the world.

JRSS Implementation Did Not Achieve Other JIE Outcomes for Regional Security

~~(U//FOUO)~~ Although implementing the JRSS is reducing the footprint and number of enemy attack vectors to the DoDIN, the JRSS did not achieve other JIE outcomes for implementing regional security. [redacted]

Air Force Operators Did Not Receive Timely Access to Information

~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ [redacted]

[13] DISA officials migrated 144 installations to the JRSS (144-13=131).

~~(U//FOUO)~~ [redacted]

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

~~(U//FOUO)~~ [redacted]

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

~~(U//FOUO)~~ [redacted]

DoD Officials Did Not Ensure That the JRSS Met Users' Needs and Train JRSS Operators Before Deployment

DoD officials did not ensure that all JRSS tools met users' needs and that JRSS operators were trained prior to JRSS deployment. Because DoD officials considered the implementation of the JRSS to be a technology refresh to the existing Service-level security stacks rather than a new acquisition, DoD officials did not apply DoD Instruction 5000.02 requirements to JRSS implementation. Had DoD Instruction 5000.02 requirements been applied, DoD officials would have been required to develop and approve capability requirements, including key performance parameters, an approved test and evaluation master plan, and training for operators, all of which would have helped ensure that the product meets users' needs.

As of FY 2018, the DoD allocated approximately $1.3 billion to deploy the JRSS.

As of FY 2018, the DoD allocated approximately $1.3 billion to deploy the JRSS. The DoD CIO and DISA officials projected that the DoD would spend an additional $900 million by FY 2023 to implement the JRSS, which is $1.7 billion more than the $520 million threshold. The cost of the JRSS and its potential impact on the DoD's cybersecurity and mission effectiveness supports the need for documented and approved capability requirements and trained operators to ensure that the JRSS meets users' needs and provides the capability to support the JIE.

Although DoD CIO officials considered the implementation of the JRSS a technology refresh, the JRSS Lead Action Officer stated that DoD CIO officials considered the JRSS implementation to be a hybrid of two DISA acquisition models—enterprise services and continuous capability delivery.[14] The DISA IT Acquisition Guide states that the enterprise services model is the configuration, integration, and customization of commercial-off-the-shelf products and services for DoD-wide use. The continuous capability delivery model involves IT portfolios and programs that satisfy a long-term capability requirement on a continuous basis.

In May 2016, DoD CIO officials issued a functional requirements document for the JRSS; however, this was almost 2 years after DISA began implementing JRSS.

For the enterprise services model, DISA guidance states that DISA officials should document requirements in a capability requirements document that includes the operational need and level of performance. However, DISA officials did not develop a capability requirements document before deploying the JRSS. A DoD CIO official stated that he attempted to correct the lack of documented requirements by preparing a functional requirements document for a future version of the JRSS. Specifically, in May 2016, DoD CIO officials issued a functional requirements document for the JRSS; however, this was almost 2 years after DISA began implementing the JRSS. Furthermore, the functional requirements document did not include all of the capabilities necessary for JRSS operators to perform their duties, such as obtaining and reviewing log files to detect unauthorized activity. Therefore, the DoD CIO and DISA officials should develop a baseline JRSS functional requirement document that includes all capabilities required for the JRSS to meet user needs and the expected outcomes of implementing regional

[14] The JRSS Lead Action Officer is a DoD CIO official.

security. Once the JRSS functional capabilities requirement document is developed, DISA should establish and implement a plan to incorporate the required capabilities into the JRSS.

The DISA IT Acquisition Guide also states that DISA is responsible for defining support services it provides, including training. Specifically, the DISA IT Acquisition Guide states that DISA officials should have a strategy to ensure that the necessary resources and processes are in place to fulfill its requirements. DISA officials should document and evaluate operational support required for implementation and training. In August 2017, U.S. Cyber Command, the component responsible for developing the JRSS operational procedures, training, and exercises, issued the JRSS Operations Training Requirements Document (nearly 3 years after DISA began migrating DoD Components to the JRSS). According to the JRSS Operations Training Requirements Document, DISA will provide JRSS-specific training—which includes JRSS familiarization training, scenario-based training, and lab-based exercises—until DoD Components incorporate JRSS operational training into their institutional training. However, for the sites we visited, DISA officials did not provide JRSS-specific training to all Component JRSS operators. For example, from May 2017 through April 2018, DISA officials provided scenario-based training to only 3 of 37 Army JRSS operators and 10 of 186 Air Force JRSS operators.

According to DISA officials, beginning in May 2017, they offered JRSS scenario-based training once per month; however, the training was limited in class size and frequency due to a lack of funding for contractors to provide training, training locations, and equipment. JRSS operators need JRSS-specific training to fully execute JRSS capabilities to defend the DoDIN and enhance cybersecurity. Therefore, DISA officials should develop and implement a schedule to provide all JRSS operators with training, as required by the JRSS Operations Training Requirements Document.

For a capability of this significance and cost, regardless of whether it is considered a technology refresh, the DoD needs to establish a minimum set of acquisition guidelines to ensure that the end product meets users' needs. Therefore, the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the DoD CIO, should establish or revise guidance that requires DoD Components to follow the same requirements when developing a technology refresh that will exceed an established cost threshold, as required for new acquisitions under DoD Instruction 5000.02.

For a capability of this significance and cost, regardless of whether it is considered a technology refresh, the DoD needs to establish a minimum set of acquisition guidelines to ensure that the end product meets users' needs.

DISA Officials Did Not Remediate Critical and High Vulnerabilities on the JRSS

~~(U//FOUO)~~ DISA serves as the JRSS PMO and is responsible for identifying and successfully remediating vulnerabilities and developing a plan of action and milestones for vulnerabilities that cannot be remediated. [redacted][15]

To determine whether DISA officials remediated known critical and high vulnerabilities, we reviewed the results of ACAS scans conducted between May 2017 and March 2018. [redacted]

[15] Critical and high vulnerabilities are vulnerabilities that would allow adversaries to directly and immediately compromise the confidentiality, integrity, or availability of systems and data.

Table 2. ~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ ID	Description	Days on System
1	[redacted]	[redacted]
2	[redacted]	[redacted]
3	[redacted]	[redacted]
4	[redacted]	[redacted]
5	[redacted]	[redacted]
6	[redacted]	[redacted]
7	[redacted]	[redacted]
8	[redacted]	[redacted]
9	[redacted]	[redacted]
10	[redacted]	[redacted]
11	[redacted]	[redacted]
12	[redacted]	[redacted]
13	[redacted]	[redacted]
14	[redacted]	[redacted] ~~(U//FOUO)~~

[1] ~~(U//FOUO)~~ [redacted]

[2] ~~(U//FOUO)~~ [redacted]

[3] ~~(U//FOUO)~~ [redacted]

[4] ~~(U//FOUO)~~ [redacted]

Source: The DoD OIG.

~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ Critical and high vulnerabilities could result in a total loss of information or provide an attacker with immediate access into or within a system. [redacted]

Critical and high vulnerabilities could result in a total loss of information or provide an attacker with immediate access into or within a system.

~~(U//FOUO)~~ The JRSS Program Management Officer did not ensure that DISA officials remediated vulnerabilities in accordance with the JRSS Vulnerability Management Plan. The JRSS vulnerability management guidance states that the JRSS PMO is responsible for directing the vulnerability management process, which includes identifying and successfully remediating vulnerabilities and developing plans of action and milestones for vulnerabilities that DISA officials cannot remediate. Furthermore, the JRSS Program Management Officer is responsible for overseeing the JRSS vulnerability management program. Identifying and correcting vulnerabilities significantly reduces the opportunities for exploitations. [redacted]

Achieving JIE Vision Requires an Operationally Effective JRSS

According to the Director of DoDIN Modernization, the JRSS is the most critical near-term element of the DoD's JIE. Therefore, if the JRSS is not operationally effective, secure, and sustainable, the DoD may not achieve the JIE vision, which includes achieving greater security on the DoDIN. In addition, without adequate security safeguards for the JRSS, weaknesses identified in this report could prevent network defenders from obtaining the information necessary to make timely decisions, and could lead to unauthorized access to the DoDIN and the destruction, manipulation, or compromise of DoD data.

Management Actions Taken

In December 2018, the DoD CIO issued a memorandum describing actions that the DoD CIO plans to take to improve JRSS operations. The DoD CIO issued the memorandum in response to recommendations the Director of Operational Test and Evaluation made in an annual report in December 2018. The Director of Operational Test and Evaluation oversaw the March 2018 operational assessment. In the testing report, the Director of Operational Test and Evaluation made the following recommendations.

- The DoD CIO and the Services should stop deploying the JRSS until the JRSS can demonstrate the capability to help network defenders detect and respond to operationally realistic cyber attacks.
- DISA and the Services should ensure that sufficient trained personnel are available to support JRSS migration schedules.
- The DoD CIO and the Services should determine whether the data flow designed to pass through each JRSS is too large to enable secure data management and, if so, refine JRSS deployment plans to reduce the data flow.
- DISA and the Services should conduct routine cyber assessments of deployed JRSSs to discover and address critical cyber vulnerabilities.

In the December 2018 memorandum, the DoD CIO stated that the pace of JRSS migrations would be delayed until known issues were resolved. He also stated that the JRSS PMO was analyzing potential changes to the architecture to address the data flow and other performance issues. The DoD CIO stated that the JRSS PMO established a virtual instance of the JRSS in the cybersecurity range and developed training curriculum required to improve operator proficiency.[16] Furthermore, the DoD CIO stated that he would collaborate with U.S. Cyber Command and DISA to further evaluate the actions required to establish a Persistent Cyber Opposing Force.[17]

Although the DoD CIO's memorandum addressed training challenges as identified in this report, it did not specify whether the DoD CIO will require DISA to develop and implement a schedule for providing all JRSS operators with JRSS scenario-based training and lab-based exercises. Therefore, we are making a JRSS training recommendation to the DISA Director, who is responsible for providing training

[16] According to the DoD CIO and JRSS PMO personnel, a virtual instance is defined as a hands-on cyber training capability that allows JRSS operators to become familiar with the JRSS without impacting production traffic.

[17] According to the DoD CIO and JRSS PMO personnel, the Persistent Cyber Opposing Force is a Red Team that will establish an ongoing presence and serve as the adversary against a cyber-defense capability.

and technical support and overseeing network and security services, to develop and implement a schedule to provide all JRSS operators with training to include JRSS scenario-based training and lab-based exercises.

~~(U//FOUO)~~ In addition, during our audit, we informed the JRSS PMO that some capabilities were not meeting users' needs. [redacted]

Management Comments on the Finding and Our Response

DoD Chief Information Officer and Director of the Defense Information Systems Agency Comments on JRSS Capabilities

~~(U//FOUO)~~ The Principal Deputy CIO, responding for the DoD CIO, and the DISA Director both stated that the DoD took action to address our findings. [redacted]

Our Response

~~(U//FOUO)~~ We were informed of the January 2019 Operations Rehearsal during our exit conference with the Office of the Under Secretary of Defense for Acquisition and Sustainment, DoD CIO, and DISA on January 23, 2019. However, DISA did not provide the results of the Rehearsal until we received their management comments on May 2, 2019. [redacted] After reviewing that documentation, we determined that [redacted]

DoD Chief Information Officer and Director of the Defense Information Systems Agency Comments on JRSS Operator Training

The Principal Deputy CIO, responding for the DoD CIO, stated that the DoD improved the training capabilities and capacity of scenario-based training. According to the DISA Director, the number of trained operators referenced in the report is not indicative of the total number of operators trained. Specifically, from May 2017 to April 2018, DISA offered 384 seats in scenario-based training courses and, of the 384 available seats, the Army and Air Force filled 70 and 65 seats, respectively.

Our Response

The number of JRSS operators identified in this report having received scenario-based training, is specific to the sites we visited—Fort Huachuca, Arizona; Gunter Annex, Alabama; and Joint Base San Antonio, Texas. To determine the number of JRSS operators that received scenario-based training, we obtained a list of all operators at those sites. After analyzing the list, we determined that 37 Army operators were located at Fort Huachuca and 186 Air Force operators were located at Gunter Annex and Joint Base San Antonio. Subsequently, the JRSS PMO provided a list of scenario-based training participants. We compared the list of Army and Air Force operators from Fort Huachuca, Gunter Annex, and Joint Base San Antonio to the list of scenario-based training participants. Based on that comparison, we determined that, for the sites we visited, only 3 of 37 Army operators and 10 of 186 Air Force operators received scenario-based training.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the DoD Chief Information Officer, establish or revise guidance that requires DoD Components to follow the same requirements when developing a technology refresh that will exceed an established cost threshold, as required for new acquisitions under DoD Instruction 5000.02.

Under Secretary of Defense for Acquisition and Sustainment Comments

The Assistant Secretary of Defense for Acquisition, responding for the Under Secretary of Defense for Acquisition and Sustainment, agreed with the intent of our recommendation to rigorously manage technology refresh programs, but not to establish a fixed threshold that would require all such programs to be managed as "new programs." The Assistant Secretary stated that future DoD information systems and commercial off-the-shelf hardware acquisitions will be guided by policy designed for the unique characteristics of information systems and commercial off-the-shelf hardware. The Assistant Secretary stated that these policies are in development and that the Office of the Under Secretary of Defense for Acquisition and Sustainment will consider the intent of the recommendation in that context.

Our Response

Although the Assistant Secretary partially agreed with the recommendation, the proposed actions to establish guidance for DoD information systems and commercial-off-the-shelf acquisitions did not address all specifics of the recommendation. DoD Instruction 5000.02 provides guidance to manage and oversee DoD acquisitions. For example, DoD Instruction 5000.02 states that:

> The structure of a DoD acquisition program and the procedures used should be tailored as much as possible to the characteristics of the product being acquired, and to the totality of circumstances associated with the program including operational urgency and risk factors. Milestone Decision Authorities will tailor program strategies and oversight, including program information, acquisition phase content, the timing and scope of decision reviews and decision levels, based on the specifics of the product being acquired, including complexity, risk factors, and required timelines to satisfy validated capability requirements.

DoD Instruction 5000.02 does not provide management and oversight requirements for the implementation of technology refreshes. Had the DoD Instruction 5000.02 provided guidance for technology refreshes that exceed the established cost threshold, DoD officials would have been required to document capability requirements, identify products and services that may satisfy those requirements, and test the operational effectiveness, suitability, and security of those products and services before deploying the JRSS. While the Assistant Secretary's comments identified the need for rigorous management of future technology refreshes, the comments did not explain how the new guidance will address the processes and procedures that should be followed when acquiring technology refreshes. Therefore, the recommendation is unresolved. We request additional comments from the Under Secretary of Defense for Acquisition and Sustainment explaining how the new guidance will address processes and procedures that must be followed when acquiring technology refreshes.

Recommendation 2

We recommend that the DoD Chief Information Officer, in coordination with the Defense Information Systems Agency Director, develop a baseline Joint Regional Security Stacks functional capabilities requirement document that includes all capabilities required for the Joint Regional Security Stacks to meet user needs and the expected outcomes of implementing regional security.

DoD Chief Information Officer Comments

The Principal Deputy CIO, responding for the DoD CIO, disagreed, stating that the DoD developed a JRSS 2.0 functional requirements document that was fully coordinated with all stakeholders, endorsed by the Joint Information Environment Executive Committee, and approved by the DoD CIO. The Principal Deputy stated that the DoD also developed JRSS measures of effectiveness (MoE) and measures of performance (MoP) that provide detailed performance criteria and associated threshold values for the critical operational issues. According to the Principal Deputy, the functional requirements document and the MoEs and MoPs are sufficient to meet user needs and the expected outcomes of implementing JRSS 2.0. However, the Principal Deputy stated that the DoD CIO will coordinate with U.S. Cyber Command, Joint Force Headquarters–DoD Information Network, and DISA to review and, if required, update the JRSS MoEs and MoPs to reflect joint operational requirements; map the JRSS functional requirements document to the MoEs and MoPs; and add an appendix to the functional requirements document to include the MoEs and MoPs. The Principal Deputy stated that the DoD CIO will complete these actions by December 2019.

Our Response

Although the Principal Deputy disagreed, the proposed actions to map the JRSS functional requirements document to the MoEs and MoPs and add an appendix to the functional requirements document to include the MoEs and MoPs will address the need to identify all capabilities and the levels of performance for each capability. Therefore, the proposed actions addressed all specifics of the recommendation. The recommendation is resolved and we will close it once we verify that the updated JRSS functional requirements document includes an appendix that maps all capabilities to the MoEs and MoPs.

Recommendation 3

We recommend that the Defense Information Systems Agency Director direct the Joint Regional Security Stacks Program Management Officer to:

a. **Establish and implement a plan to incorporate the required capabilities into the Joint Regional Security Stacks once the functional capabilities requirement document is developed.**

Director of Defense Information Systems Agency Comments

The DISA Director agreed, stating that DISA will continue to implement performance enhancements identified during a strategic review of the JRSS in 2018, and will support developing and fielding JRSS Next Generation. According to the Director, DISA will use the JRSS MoP criteria to evaluate technical and operational effectiveness and will propose a plan of action and milestones to address the performance gaps identified 60 days after completion of the MoP assessment.

Our Response

The DISA Director's comments addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we verify that the plan of action and milestones addresses the performance gaps identified in the MoP assessment.

b. **Develop and implement a schedule to provide all Joint Regional Security Stacks operators with training, as required by the JRSS Operations Training Requirements Document.**

Director of Defense Information Systems Agency Comments

The DISA Director agreed, stating that DISA is committed to continuing to provide the training documented in the Training Requirements Document. The Director stated that DISA posted computer-based JRSS familiarization training modules, which are available 24 hours a day; scheduled scenario-based training classes twice per month with a maximum of 32 seats per class for FY 2019; and scheduled periodic lab-based training in preparation for operational assessments. According to the Director, DISA will work with U.S. Cyber Command, the DoD CIO, and the DoD Components to expedite incorporating JRSS operational training requirements into the Components' institutional training programs using best practices.

Our Response

The Director's comments addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we verify that the JRSS familiarization training is accessible 24 hours a day and that the scenario and lab-based training has been scheduled as stated. We will review the

Service and agency training program schedules when the Director completes her coordination with U.S. Cyber Command, the DoD CIO, and the DoD Components that incorporate the JRSS training into the Service and agency institutional training programs.

c. ~~(U//FOUO)~~ [redacted]

Director of Defense Information Systems Agency Comments

~~(U//FOUO)~~ [redacted]

Our Response

~~(U//FOUO)~~ The Director's comments addressed all specifics of the recommendation; therefore, the recommendation is resolved. [redacted]

Appendix

Scope and Methodology

We conducted this performance audit from January 2018 through March 2019 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To determine whether the DoD's deployment of the JRSS is achieving the expected outcomes for implementing regional security, we interviewed officials from DISA Headquarters, DoD CIO, DISA Global Operations Command, U.S. Cyber Command, Army, and Air Force. We did not review the Navy because Navy officials delayed migrating to the JRSS due to the technical and latency issues that the Army and Air Force were experiencing. We reviewed applicable DoD and Federal criteria related to information systems. In addition, we reviewed the JRSS Implementation Plan, concept of operations, service operations annexes, the JRSS Training Requirements, and the JRSS certification and accreditation package.

The primary audit locations were the Pentagon, Washington, D.C.; Fort Meade, Maryland; Gunter Annex, Montgomery, Alabama; Fort Huachuca, Arizona; and Scott Air Force Base, Illinois.[18]

Use of Computer-Processed Data

We obtained vulnerability scans from the DoD ACAS system to assess whether vulnerabilities were managed and mitigated. ACAS is a network-based security compliance and assessment system designed to provide awareness of the security posture and network health of DoD networks. We determined that the ACAS scan reports were sufficient and reliable to support the finding that vulnerabilities were not remediated in accordance with guidance. We did not assess the DoD ACAS systems controls.

[18] The operators who manage the security stacks at Fort Bragg, North Carolina, and Joint Base San Antonio, Texas, are physically located at Fort Huachuca, Arizona, and Gunter Annex, Alabama, respectively.

Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) issued one report discussing JIE implementation related to the JRSS.

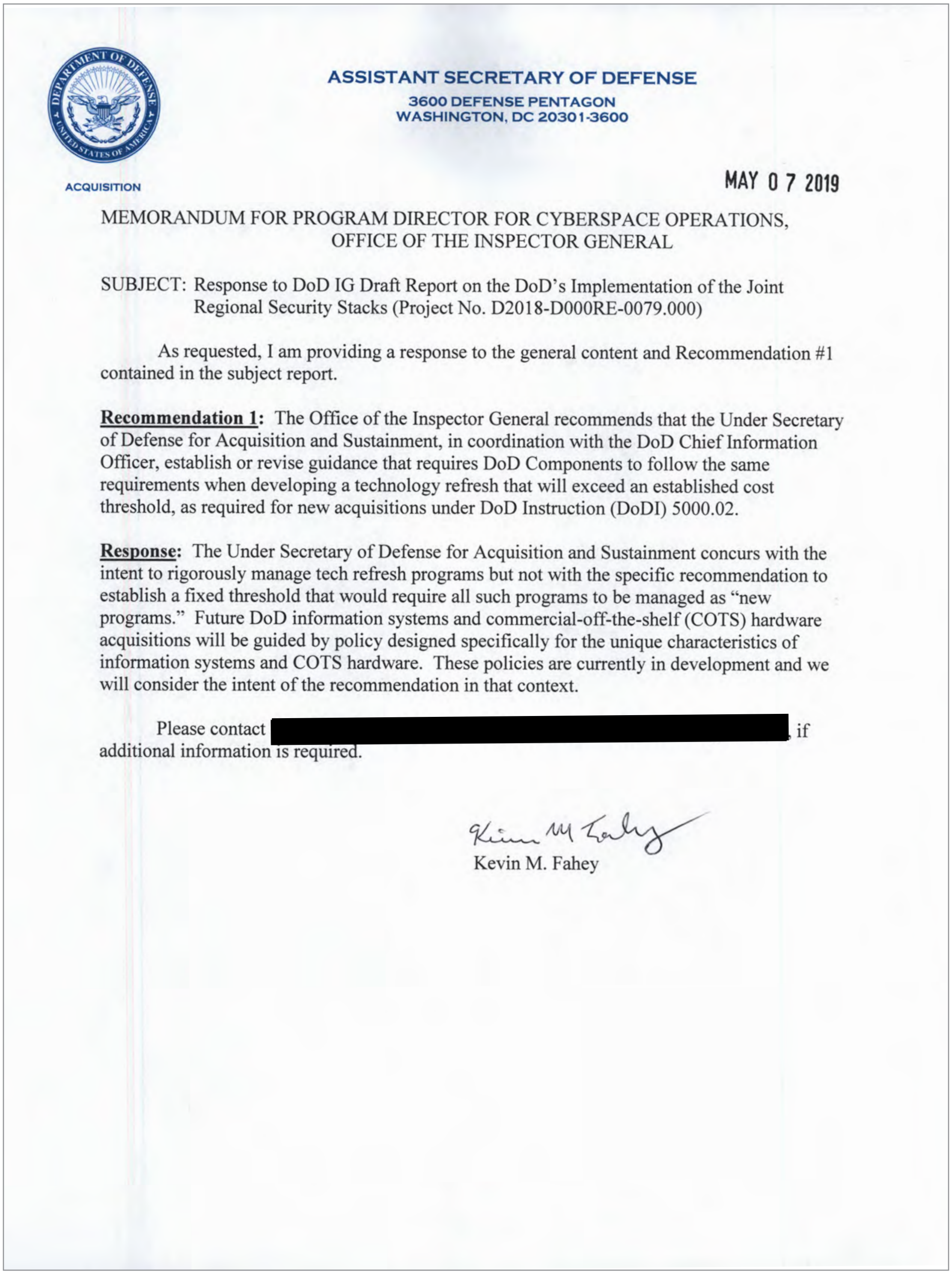
GAO

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

> The GAO found that the DoD had not determined the number of staff and the specific skills and abilities needed to operate the JIE. The DoD also lacked a strategy to ensure that required JIE security assessments were conducted. The GAO recommended that the DoD fully define the JIE's scope and expected cost, and take steps to improve workforce and security planning.

Management Comments

Under Secretary of Defense for Acquisition and Sustainment



ASSISTANT SECRETARY OF DEFENSE
3600 DEFENSE PENTAGON
WASHINGTON, DC 20301-3600

ACQUISITION

MAY 07 2019

MEMORANDUM FOR PROGRAM DIRECTOR FOR CYBERSPACE OPERATIONS, OFFICE OF THE INSPECTOR GENERAL

SUBJECT: Response to DoD IG Draft Report on the DoD's Implementation of the Joint Regional Security Stacks (Project No. D2018-D000RE-0079.000)

As requested, I am providing a response to the general content and Recommendation #1 contained in the subject report.

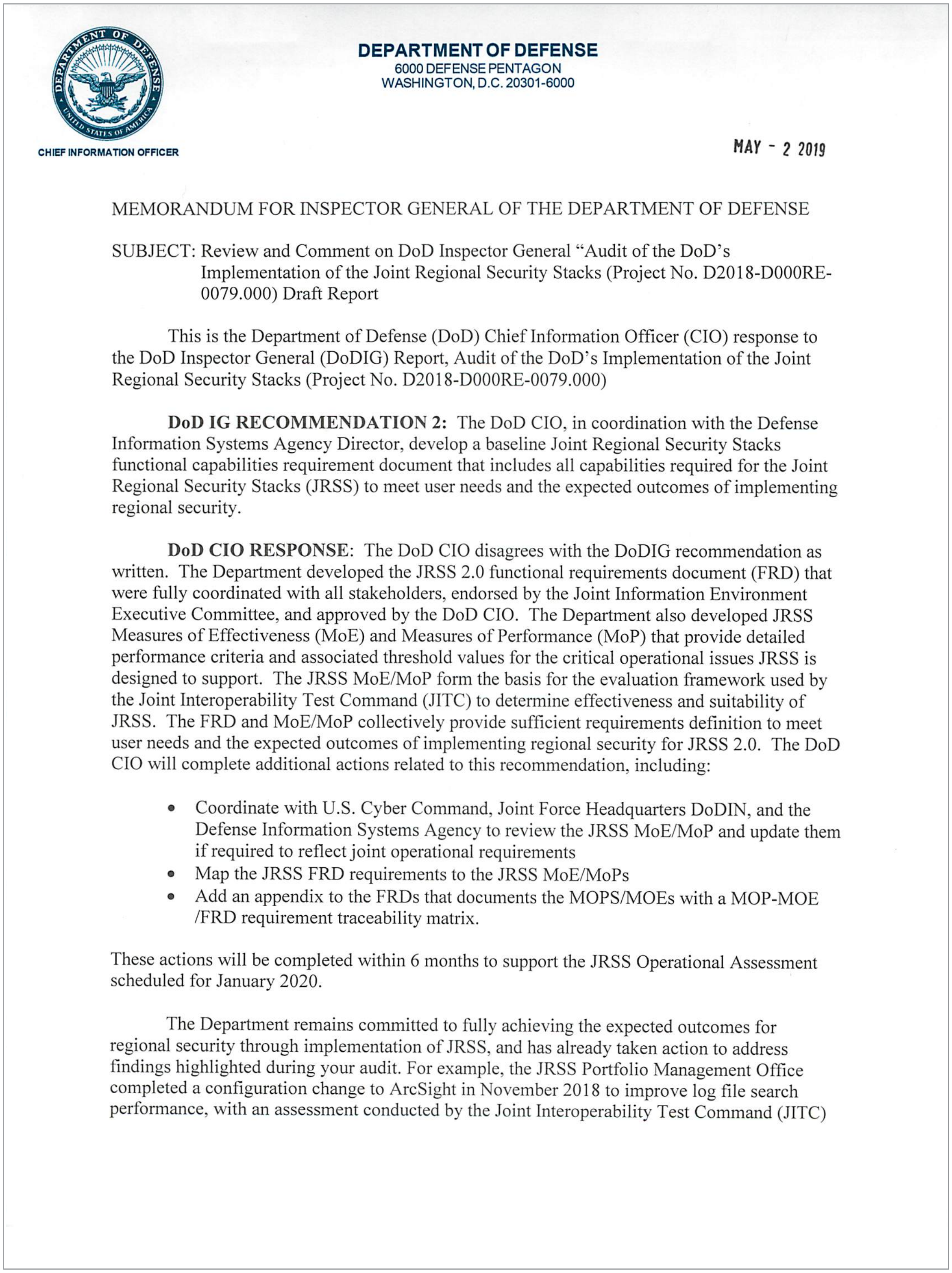
Recommendation 1: The Office of the Inspector General recommends that the Under Secretary of Defense for Acquisition and Sustainment, in coordination with the DoD Chief Information Officer, establish or revise guidance that requires DoD Components to follow the same requirements when developing a technology refresh that will exceed an established cost threshold, as required for new acquisitions under DoD Instruction (DoDI) 5000.02.

Response: The Under Secretary of Defense for Acquisition and Sustainment concurs with the intent to rigorously manage tech refresh programs but not with the specific recommendation to establish a fixed threshold that would require all such programs to be managed as "new programs." Future DoD information systems and commercial-off-the-shelf (COTS) hardware acquisitions will be guided by policy designed specifically for the unique characteristics of information systems and COTS hardware. These policies are currently in development and we will consider the intent of the recommendation in that context.

Please contact [redacted], if additional information is required.

Kevin M. Fahey

DoD Chief Information Officer



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

MAY - 2 2019

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Review and Comment on DoD Inspector General "Audit of the DoD's Implementation of the Joint Regional Security Stacks (Project No. D2018-D000RE-0079.000) Draft Report

This is the Department of Defense (DoD) Chief Information Officer (CIO) response to the DoD Inspector General (DoDIG) Report, Audit of the DoD's Implementation of the Joint Regional Security Stacks (Project No. D2018-D000RE-0079.000)

DoD IG RECOMMENDATION 2: The DoD CIO, in coordination with the Defense Information Systems Agency Director, develop a baseline Joint Regional Security Stacks functional capabilities requirement document that includes all capabilities required for the Joint Regional Security Stacks (JRSS) to meet user needs and the expected outcomes of implementing regional security.

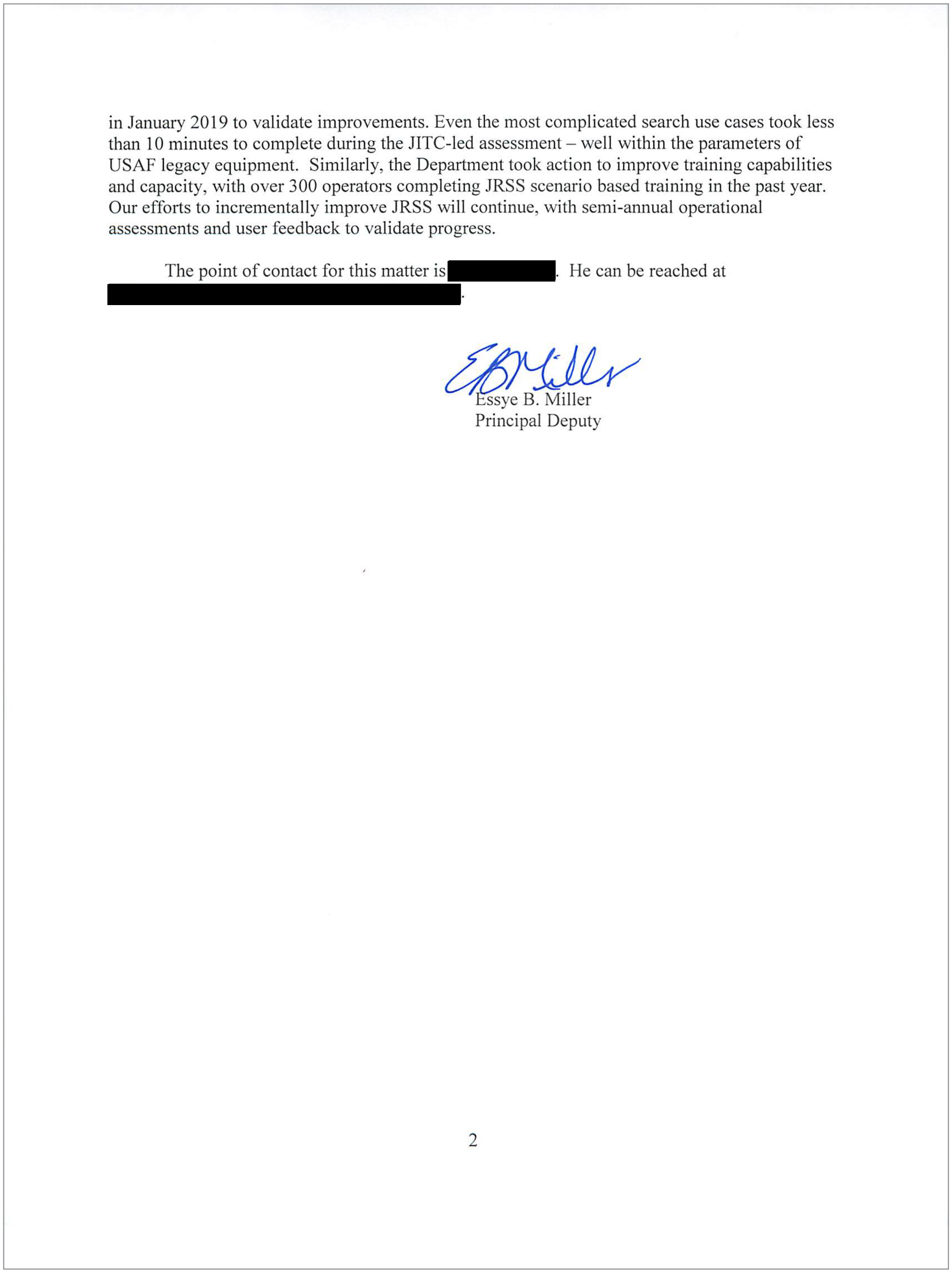
DoD CIO RESPONSE: The DoD CIO disagrees with the DoDIG recommendation as written. The Department developed the JRSS 2.0 functional requirements document (FRD) that were fully coordinated with all stakeholders, endorsed by the Joint Information Environment Executive Committee, and approved by the DoD CIO. The Department also developed JRSS Measures of Effectiveness (MoE) and Measures of Performance (MoP) that provide detailed performance criteria and associated threshold values for the critical operational issues JRSS is designed to support. The JRSS MoE/MoP form the basis for the evaluation framework used by the Joint Interoperability Test Command (JITC) to determine effectiveness and suitability of JRSS. The FRD and MoE/MoP collectively provide sufficient requirements definition to meet user needs and the expected outcomes of implementing regional security for JRSS 2.0. The DoD CIO will complete additional actions related to this recommendation, including:

- Coordinate with U.S. Cyber Command, Joint Force Headquarters DoDIN, and the Defense Information Systems Agency to review the JRSS MoE/MoP and update them if required to reflect joint operational requirements
- Map the JRSS FRD requirements to the JRSS MoE/MoPs
- Add an appendix to the FRDs that documents the MOPS/MOEs with a MOP-MOE /FRD requirement traceability matrix.

These actions will be completed within 6 months to support the JRSS Operational Assessment scheduled for January 2020.

The Department remains committed to fully achieving the expected outcomes for regional security through implementation of JRSS, and has already taken action to address findings highlighted during your audit. For example, the JRSS Portfolio Management Office completed a configuration change to ArcSight in November 2018 to improve log file search performance, with an assessment conducted by the Joint Interoperability Test Command (JITC)

DoD Chief Information Officer (cont'd)

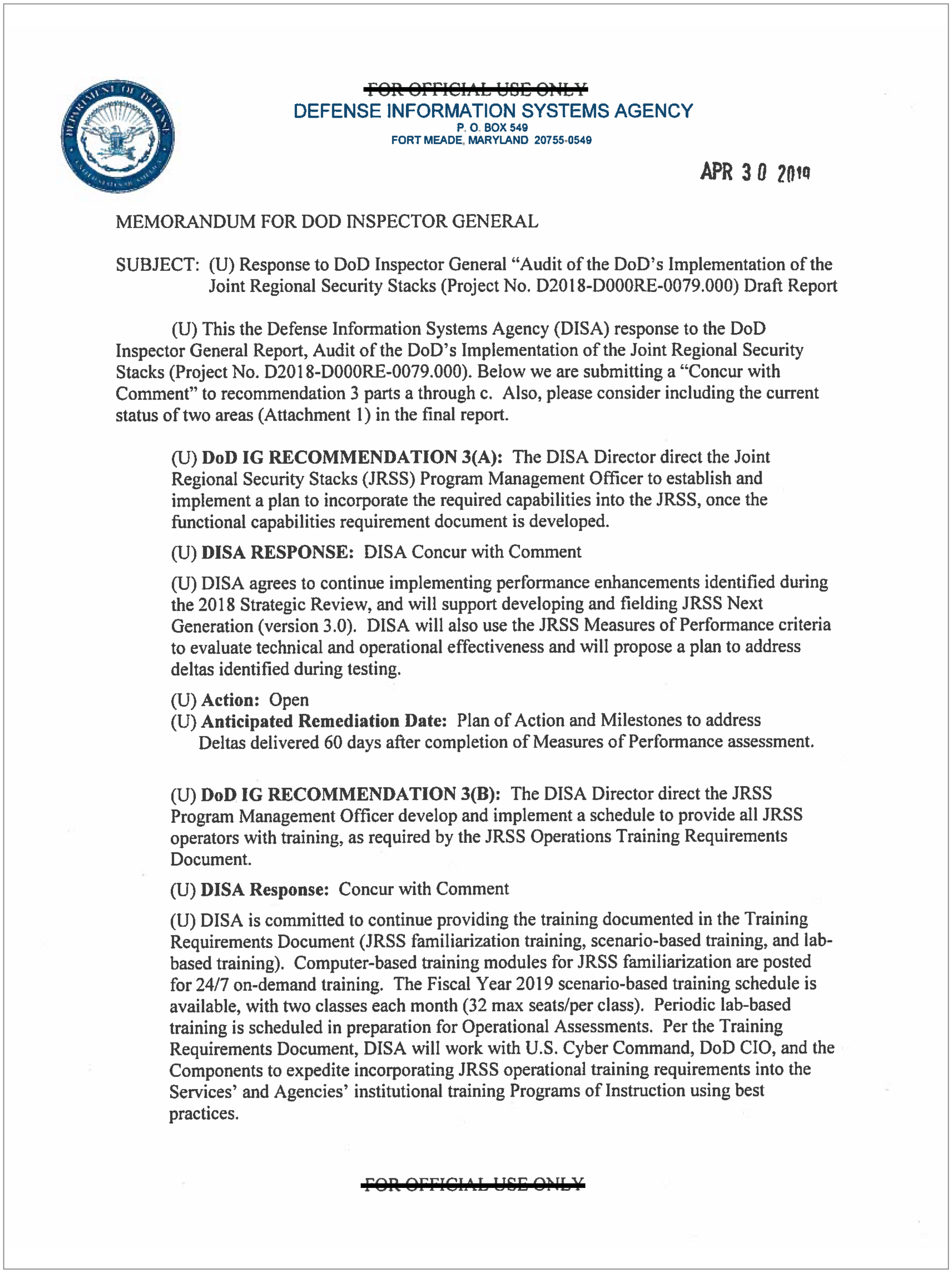


in January 2019 to validate improvements. Even the most complicated search use cases took less than 10 minutes to complete during the JITC-led assessment – well within the parameters of USAF legacy equipment. Similarly, the Department took action to improve training capabilities and capacity, with over 300 operators completing JRSS scenario based training in the past year. Our efforts to incrementally improve JRSS will continue, with semi-annual operational assessments and user feedback to validate progress.

The point of contact for this matter is [redacted]. He can be reached at [redacted].

Essye B. Miller
Principal Deputy

Defense Information Systems Agency



~~FOR OFFICIAL USE ONLY~~

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

APR 30 2019

MEMORANDUM FOR DOD INSPECTOR GENERAL

SUBJECT: (U) Response to DoD Inspector General "Audit of the DoD's Implementation of the Joint Regional Security Stacks (Project No. D2018-D000RE-0079.000) Draft Report

(U) This the Defense Information Systems Agency (DISA) response to the DoD Inspector General Report, Audit of the DoD's Implementation of the Joint Regional Security Stacks (Project No. D2018-D000RE-0079.000). Below we are submitting a "Concur with Comment" to recommendation 3 parts a through c. Also, please consider including the current status of two areas (Attachment 1) in the final report.

(U) **DoD IG RECOMMENDATION 3(A):** The DISA Director direct the Joint Regional Security Stacks (JRSS) Program Management Officer to establish and implement a plan to incorporate the required capabilities into the JRSS, once the functional capabilities requirement document is developed.

(U) **DISA RESPONSE:** DISA Concur with Comment

(U) DISA agrees to continue implementing performance enhancements identified during the 2018 Strategic Review, and will support developing and fielding JRSS Next Generation (version 3.0). DISA will also use the JRSS Measures of Performance criteria to evaluate technical and operational effectiveness and will propose a plan to address deltas identified during testing.

(U) **Action:** Open
(U) **Anticipated Remediation Date:** Plan of Action and Milestones to address Deltas delivered 60 days after completion of Measures of Performance assessment.

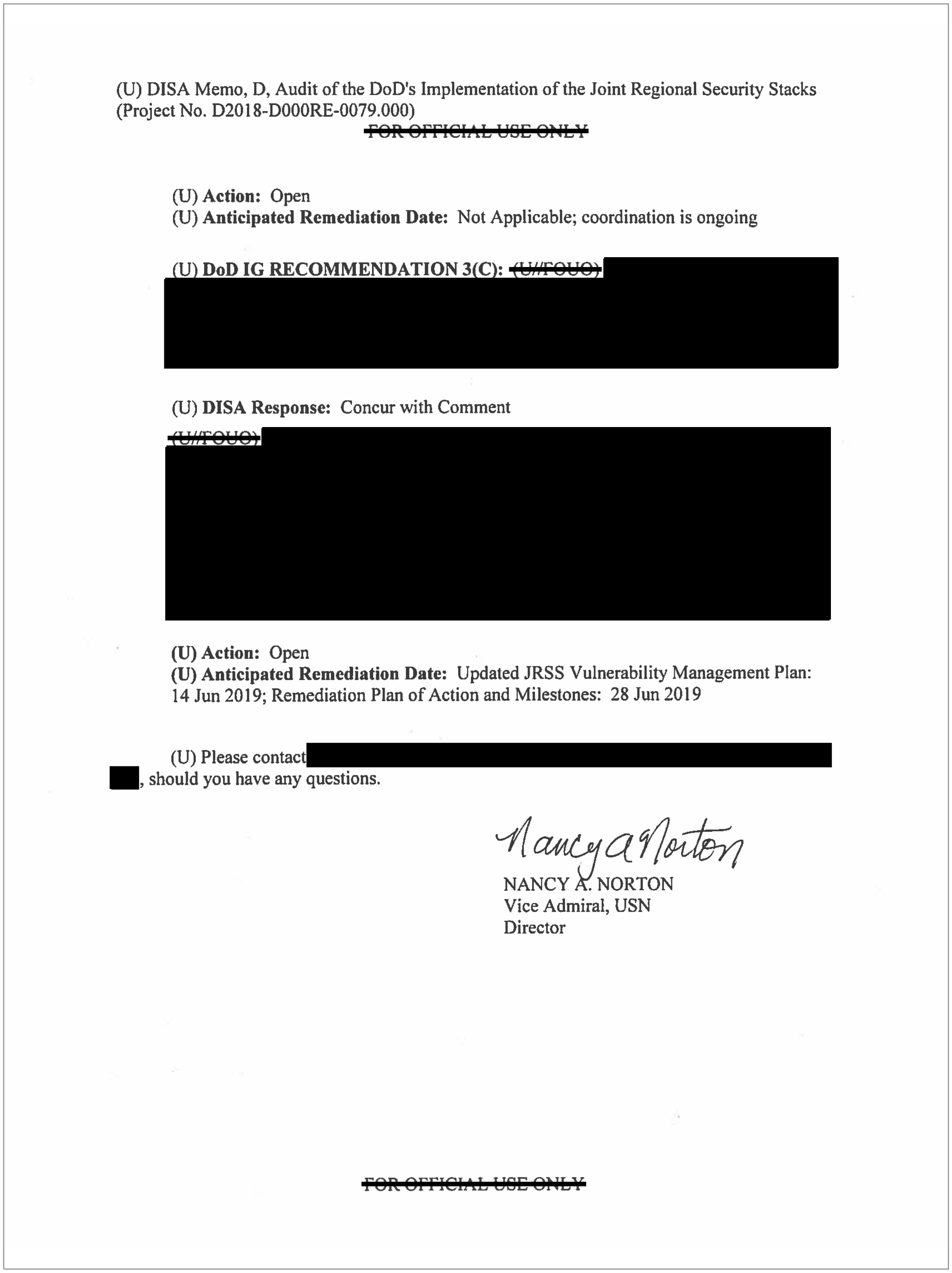
(U) **DoD IG RECOMMENDATION 3(B):** The DISA Director direct the JRSS Program Management Officer develop and implement a schedule to provide all JRSS operators with training, as required by the JRSS Operations Training Requirements Document.

(U) **DISA Response:** Concur with Comment

(U) DISA is committed to continue providing the training documented in the Training Requirements Document (JRSS familiarization training, scenario-based training, and lab-based training). Computer-based training modules for JRSS familiarization are posted for 24/7 on-demand training. The Fiscal Year 2019 scenario-based training schedule is available, with two classes each month (32 max seats/per class). Periodic lab-based training is scheduled in preparation for Operational Assessments. Per the Training Requirements Document, DISA will work with U.S. Cyber Command, DoD CIO, and the Components to expedite incorporating JRSS operational training requirements into the Services' and Agencies' institutional training Programs of Instruction using best practices.

~~FOR OFFICIAL USE ONLY~~

Defense Information Systems Agency (cont'd)



(U) DISA Memo, D, Audit of the DoD's Implementation of the Joint Regional Security Stacks (Project No. D2018-D000RE-0079.000)

~~FOR OFFICIAL USE ONLY~~

(U) **Action:** Open
(U) **Anticipated Remediation Date:** Not Applicable; coordination is ongoing

(U) **DoD IG RECOMMENDATION 3(C):** ~~(U//FOUO)~~ [redacted]

(U) **DISA Response:** Concur with Comment

~~(U//FOUO)~~ [redacted]

(U) Action: Open
(U) Anticipated Remediation Date: Updated JRSS Vulnerability Management Plan: 14 Jun 2019; Remediation Plan of Action and Milestones: 28 Jun 2019

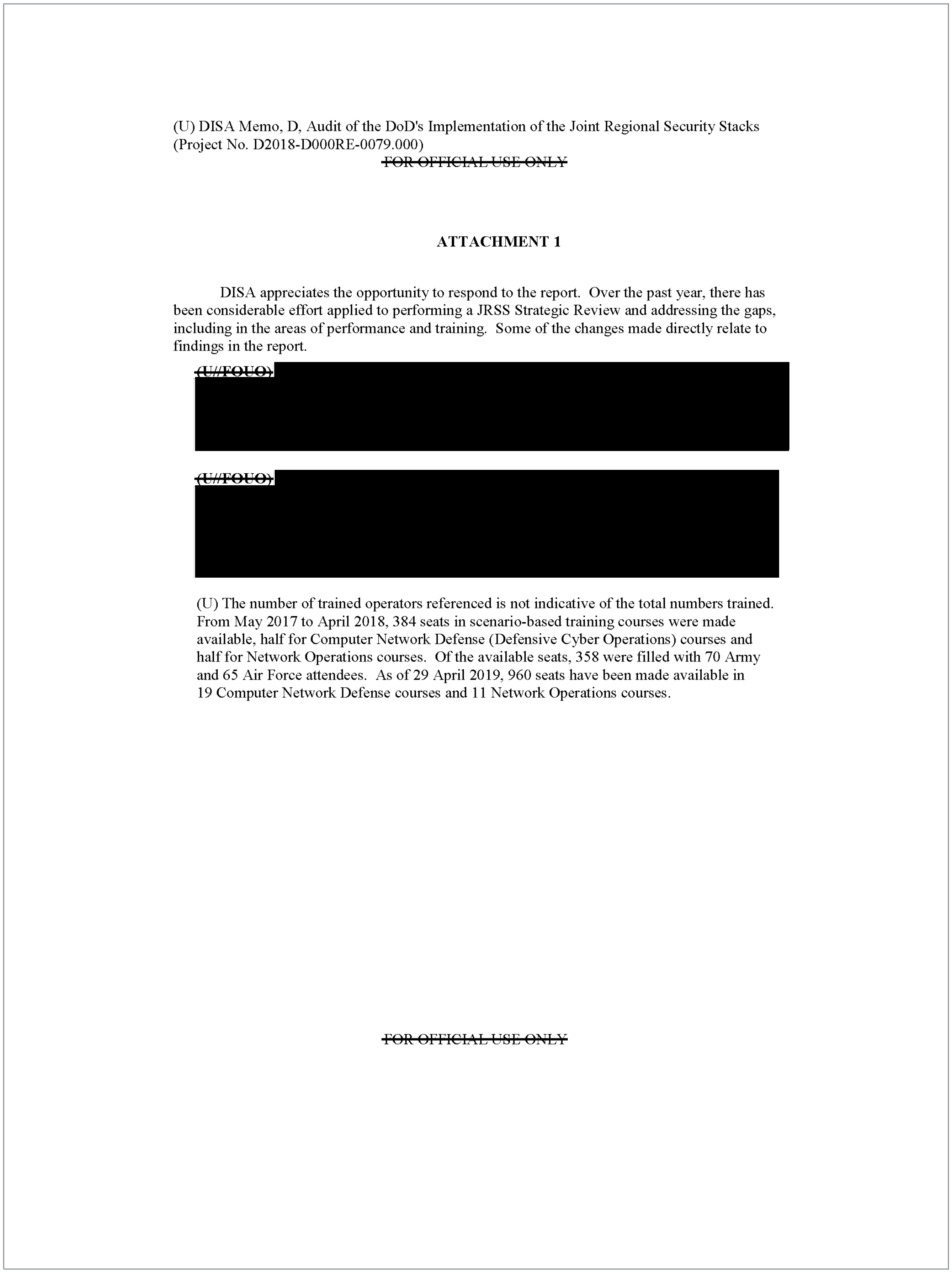
(U) Please contact [redacted], should you have any questions.

Nancy A Norton

NANCY A. NORTON
Vice Admiral, USN
Director

~~FOR OFFICIAL USE ONLY~~

Defense Information Systems Agency (cont'd)



ATTACHMENT 1

DISA appreciates the opportunity to respond to the report. Over the past year, there has been considerable effort applied to performing a JRSS Strategic Review and addressing the gaps, including in the areas of performance and training. Some of the changes made directly relate to findings in the report.

~~(U//FOUO)~~ [redacted]

~~(U//FOUO)~~ [redacted]

(U) The number of trained operators referenced is not indicative of the total numbers trained. From May 2017 to April 2018, 384 seats in scenario-based training courses were made available, half for Computer Network Defense (Defensive Cyber Operations) courses and half for Network Operations courses. Of the available seats, 358 were filled with 70 Army and 65 Air Force attendees. As of 29 April 2019, 960 seats have been made available in 19 Computer Network Defense courses and 11 Network Operations courses.

Acronyms and Abbreviations

ACAS	Assured Compliance Assessment Solution
CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DoDIN	DoD Information Network
IT	Information Technology
JIE	Joint Information Environment
JMS	Joint Management System
JRSS	Joint Regional Security Stack
MoE	Measures of Effectiveness
MoP	Measures of Performance
NIPRNET	Non-Secure Internet Protocol Router Network
PMO	Program Management Office

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