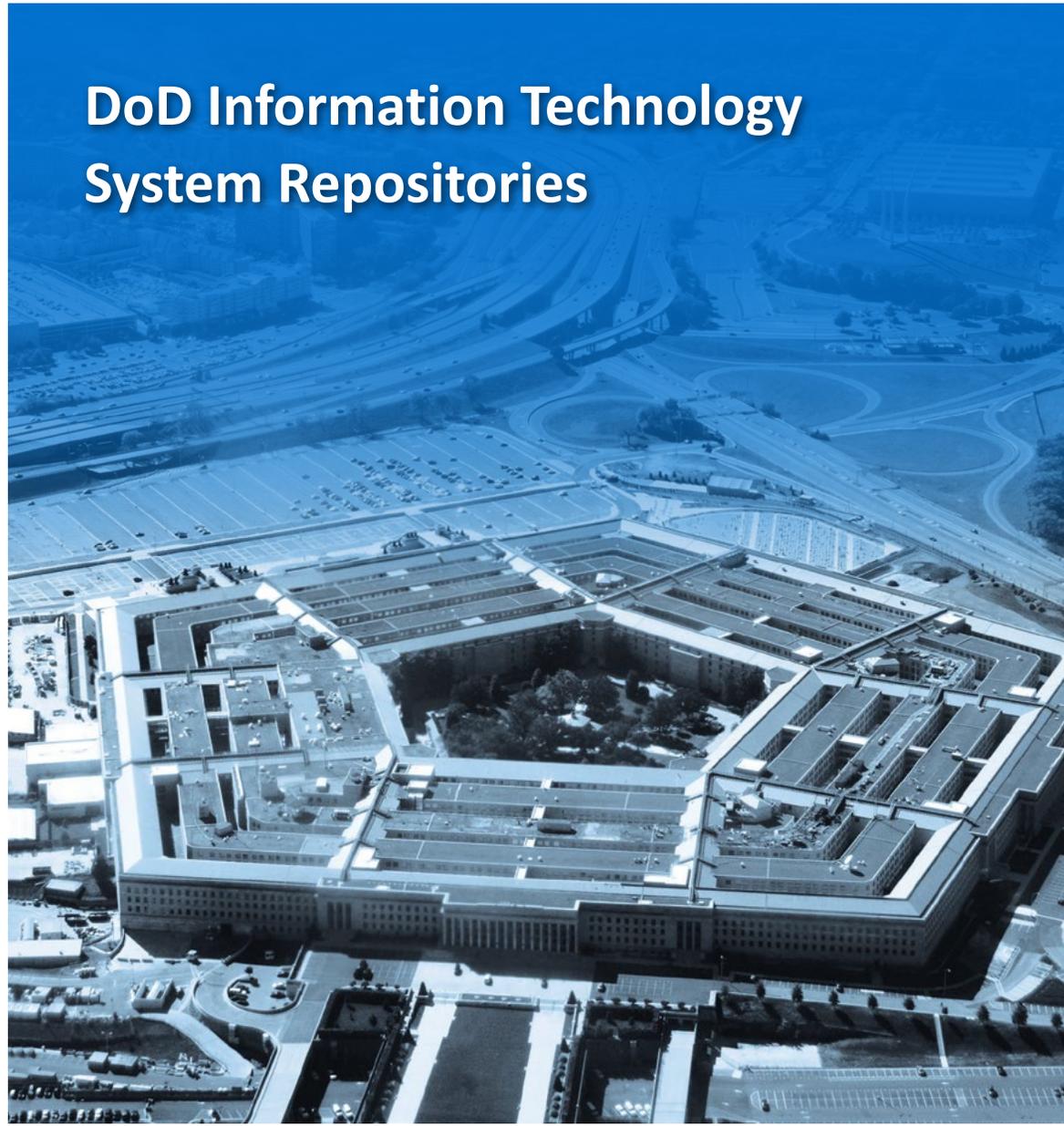




# INSPECTOR GENERAL

*U.S. Department of Defense*

SEPTEMBER 24, 2018



## DoD Information Technology System Repositories

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE





# Results in Brief

## *DoD Information Technology System Repositories*

September 24, 2018

### Objective

We determined whether DoD Components reported accurate information technology system data in the SECRET Internet Protocol Router Network (SIPRNET) Information Technology Registry (SITR).

### Background

DoD guidance states that SITR is the authoritative classified inventory of the DoD's mission-critical and mission-essential information technology systems. Mission-critical information technology systems are necessary to continue warfighter operations and direct mission support of warfighter operations, while mission-essential information technology systems are basic and necessary to accomplish an organization's mission. As of March 2017, when we selected our nonstatistical sample, SITR contained information for 199 individual information technology systems across 13 DoD Components.

### Findings

DoD Components did not report accurate or complete information technology system data in SITR for 31 of 32 information technology systems in our nonstatistical sample. This occurred because the DoD Chief Information Officer (CIO) did not have a process to notify information technology system users of inaccurate SITR data, require SITR training, or hold Component CIOs accountable for ensuring the accuracy and completeness of the data in SITR. As a result, the DoD cannot rely

### Findings (cont'd)

on SITR data for decision making as intended, which can affect stovepiped Component databases, mapping annual updates of the Business Enterprise Architecture, and making resource decisions; and the DoD may not be able to support its statutory compliance reporting designed to improve critical cybersecurity infrastructure.

Additionally, we determined that the DoD maintains similar information technology data in multiple repositories, including SITR, the DoD Information Technology Portfolio Repository (DITPR), the Enterprise Mission Assurance Support Service (eMASS), Xacta, and Archer. The eMASS, Xacta, and Archer repositories are cybersecurity management tools that are used to maintain the Risk Management Framework documentation needed to authorize information technology systems to operate on DoD networks.

Although the DoD uses the repositories to meet different requirements, the DoD has an opportunity for cost savings and efficiencies if it identifies a single enterprise solution to maintain Risk Management Framework documentation that can also be used to respond to statutory requirements such as those in the Federal Information Security Modernization Act.

As of September 2017, DoD Components had spent approximately \$10 million for Xacta and Archer, systems that duplicate eMASS functionality. On March 26, 2018, the Secretary of Defense issued a memorandum, "Be Peerless Stewards of Taxpayers' Dollars," which requested a commitment from all the DoD to exercise financial accountability on every expenditure. Minimizing duplicative information technology repositories in favor of an enterprise Risk Management Framework solution is potentially a step towards meeting that commitment.

### Recommendations

We recommend that the DoD CIO:

- establish a process to notify the information technology system users of data inaccuracies in SITR, give deadlines for corrections, and regularly follow up with DoD Components to ensure resolution;



# Results in Brief

## *DoD Information Technology System Repositories*

### **Recommendations (cont'd)**

- require SITR training for all SITR and information technology system users to increase awareness of SITR's purpose, statutory requirements, and the importance of reporting accurate and complete data;
- establish a process that holds DoD Component CIOs accountable for the accuracy and completeness of the information technology system data in SITR;
- conduct a study to determine the most effective process and information technology repository for maintaining and reporting information technology data and eliminate any duplicate processes associated with the information technology repositories;
- require DoD Components to conduct and submit a business case analysis before selecting or renewing the use of a commercial Risk Management Framework accreditation and authorization tool rather than eMASS;
- develop a process to evaluate and approve DoD Components' business case analysis for the use of a commercial Risk Management Framework accreditation and authorization tool rather than eMASS; and
- require all DoD Components to use eMASS when the DoD develops the capability for eMASS to maintain top secret information technology system data.

### **Management Actions Taken**

On July 14, 2017, the DoD CIO issued a memorandum that implements a quarterly review process for SITR. The memorandum also states that the DoD CIO will send the Component CIOs a report identifying specific records and fields in SITR that contain questionable data or are missing data. Furthermore, in January 2018 the

DoD CIO initiated a training program for all SITR users. Available on the SITR website, the training defines the data that users are required to report in SITR and the importance of reporting accurate and complete data in SITR.

We consider the DoD CIO's memorandum and the SITR training program to have addressed our recommendations pertaining to reporting complete and accurate data in SITR. Therefore, the recommendations are resolved, but will remain open. We will close the recommendations once we verify that the DoD CIO has reviewed Components' data in SITR, notified them of any errors, provided milestones for corrections, and finalized a process to hold DoD Component CIOs accountable for the accuracy and completeness of the data in SITR. We will close the SITR training recommendation once we confirm the DoD CIO has required SITR users to take the training.

### **Management Comments and Our Response**

The Principal Deputy CIO, responding for the DoD CIO, disagreed with the recommendations pertaining to the DoD Components' use of eMASS and eliminating duplicate processes for maintaining and reporting information technology system data. However, the Principal Deputy stated that the office of the DoD CIO has initiated a reform project to account for and reduce information technology repositories, optimize cost, and improve data efficiency. The Principal Deputy also stated that through the process, a core set of reference management framework tools will be established to support Component and enterprise requirements. Therefore, the recommendation to conduct a study to determine the most effective process and information technology repository for maintaining and reporting information technology data is resolved, and we will



# Results in Brief

## *DoD Information Technology System Repositories*

### ***Management Comments (cont'd)***

close the recommendation once we verify that an effective process has been identified and that duplicate processes have been eliminated.

The Principal Deputy CIO partially addressed the recommendations concerning the DoD Components' use of business case analysis before selecting a commercial Risk Management Framework tool and did not address the recommendation to require the use of eMASS when it has the capability to maintain top secret information technology system data. Therefore, those recommendations remain unresolved.

Please see the Recommendations Table on the next page.

## Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
DoD Chief Information Officer	B.1.b, B.1.c, and B.1.d	A.1.a, A.1.b, A.1.c, and B.1.a	None

Please provide Management Comments by October 24, 2018.

**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

September 24, 2018

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER

SUBJECT: DoD Information Technology System Repositories (Report No. DODIG-2018-154)

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 on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Principal Deputy Chief Information Officer did not address the specifics of Recommendations B.1.b, B.1.c, and B.1.d; therefore, we request additional comments on those recommendations by October 24, 2018.

Please send a PDF file containing your comments on the recommendations to [audcso@dodig.mil](mailto: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  
Assistant Inspector General  
Cyberspace Operations

# Contents

---

## Introduction

Objective.....	1
Background.....	1
Review of Internal Controls.....	4

## Finding A. DoD Components Did Not Report Accurate and Complete Data in SITR..... 5

SITR Data Were Not Accurate and Complete.....	6
DoD CIO Did Not Properly Manage SITR Data Quality.....	8
SITR Data are Unreliable.....	10
Recommendations.....	10
Management Actions Taken to Ensure Accurate and Complete Data in SITR.....	11

## Finding B. The DoD Maintains Similar Information Technology System Data in Multiple Repositories..... 12

Risk Management Framework.....	12
The DoD Maintains Similar Information Technology System Data in Multiple Repositories.....	14
DoD Chief Information Officer Can Gain Efficiencies in Reporting Information Technology System Data.....	15
The DoD Can Potentially Use Information Technology Repositories More Efficiently.....	16
Recommendations, Management Comments, and Our Response.....	17

## Appendix

Scope and Methodology.....	19
Use of Computer-Processed Data.....	20
Prior Coverage.....	20

## Management Comments

DoD Chief Information Officer.....	22
------------------------------------	----

## Acronyms and Abbreviations..... 23

# Introduction

---

## Objective

Our audit objective was to determine whether DoD Components reported accurate information technology system data in the SECRET Internet Protocol Router Network (SIPRNET) Information Technology Registry (SITR).<sup>1</sup> See the Appendix for a discussion of the scope and methodology and prior audit coverage.

## Background

Section 2223, title 10, United States Code (10 U.S.C. § 2223 [2011]) requires Federal agencies to maintain a consolidated inventory of mission-critical and mission-essential information technology systems. The DoD defines mission-critical information technology systems as systems that, if lost or compromised, would stop warfighter operations or direct mission support of warfighter operations. Mission-essential information technology systems are defined as systems that are basic and necessary to accomplish an organization's mission. To meet the 10 U.S.C. § 2223 (2011) requirement, the DoD Chief Information Officer (CIO) established the DoD Information Technology Portfolio Repository (DITPR) and SITR as the authoritative inventories for DoD mission-critical and mission-essential information technology systems.<sup>2</sup> DoD guidance states that, based on the Components' determination about the classification level of the information, the Component should enter information technology system information in either DITPR or SITR.

SITR is a web-based repository designed to meet a wide variety of internal and external reporting requirements, including regularly scheduled reports required by legislative or regulatory mandates, and annual reports required by other Federal Departments. For example, the data are used to comply with the following Federal and statutory laws:

- The Privacy Act of 1974—requires each Federal agency to publish a system of records notice in the Federal Register for each system that contains personally identifiable information of U.S. citizens or lawful permanent residents.<sup>3</sup>
- The Clinger-Cohen Act of 1996—requires DoD Component CIOs to assist in capital investment evaluations and decision making for all programs that acquire information technology, including mission-critical and mission-essential systems.<sup>4</sup>

---

<sup>1</sup> According to Section 11101, title 40, U.S.C., January 3, 2012, information technology is any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data.

<sup>2</sup> Report Number DODIG-2017-082 focused on the accuracy and completeness of information in DITPR.

<sup>3</sup> 5 U.S.C. § 552a (2010).

<sup>4</sup> 40 U.S.C. § 1401 (1998).

- The E-Government Act of 2002—requires agencies to complete and approve Privacy Impact Assessments to ensure that personally identifiable information in electronic forms is collected, stored, protected, used, shared, and managed in a manner that protects privacy.<sup>5</sup>
- The Federal Information Security Modernization Act of 2014 (FISMA)—requires each Federal agency to evaluate and test the effectiveness of its information security programs.<sup>6</sup>

### ***SITR Data Fields***

DoD Component information technology system users enter information technology system data directly into SITR, which is divided into core and noncore data fields.

The core data fields include:

- system name—the official full name of the information technology system;
- system description—a high level summary of what the information technology system supports and the type of information it contains;
- responsible DoD Component—the DoD Component that owns and maintains the information technology system;
- mission criticality—assigned based on the value of an information technology system to DoD missions;
- acquisition category—assigned to facilitate decision making and execution, and compliance with statutory requirements, which determine the level of review, decision authority, and applicable procedures for the information technology system; and
- system interfaces—identifies whether the information technology system connects with other information technology systems.

The noncore data fields contain FISMA and Electronic-Authentication (E-Authentication) data. The FISMA data fields include:

- accreditation status—the type of authorization an information technology system has been granted to operate on a DoD network;
- accreditation date—the date the information technology system was authorized to operate on a DoD network;
- accreditation vehicle—the method used to determine whether the information technology system should be granted an authorization to operate on a DoD network;<sup>7</sup>

---

<sup>5</sup> According to Public Law 107-347, “E-Government Act of 2002,” section 208, “Privacy Provisions,” the Privacy Impact Assessment must address what information is to be collected, why the information is being collected, the intended use of the information, with whom the information will be shared, and what notice would be provided to individuals regarding what information is collected and how that information is shared.

<sup>6</sup> 44 U.S.C. § 3551 (2014).

<sup>7</sup> For system accreditation, the DoD is transitioning from the DoD Information Assurance Certification and Accreditation Process to the Risk Management Framework process. Risk Management Framework is the DoD’s integrated enterprise-wide structure for cyber security risk management.

- security control test—the date the information technology system’s security controls were last tested; and
- contingency plan—whether or not the information technology system requires a contingency plan.<sup>8</sup>

E-Authentication is the process of establishing confidence in user identities before allowing access to an information technology system. E-Authentication methods include passwords, challenge questions, tokens, and biometrics, such as fingerprints or eye scans. The E-Authentication data fields include:

- browser-based—indicates whether the information technology system is accessible from the internet;
- external facing—indicates whether the information technology system has users that are not affiliated with the DoD; and
- end-user authentication required—indicates whether users are required to authenticate their identity to access all or parts of the information technology system.

### ***SITR Data Input***

As of March 24, 2017, DoD Components had entered data into SITR for 199 information technology systems (see Table 1 for the number of systems by DoD Component). We selected a nonstatistical sample of 32 of the 199 information technology systems to review during our audit. We reviewed information technology systems from the U.S. Special Operations Command (USSOCOM) and the U.S. Indo-Pacific Command (USINDOPACOM) because they reported the highest number of information technology systems in SITR.

*Table 1. Number of Information Technology Systems in SITR as of March 24, 2017*

Component	Number of Systems in SITR
U.S. Indo-Pacific Command	96
U.S. Special Operations Command	37
U.S. Southern Command	20
U.S. Central Command	12
Joint Improvised-Threat Defeat Organization	12
U.S. European Command	7
National Geospatial-Intelligence Agency	5

<sup>8</sup> If certification and accreditation are required, Components must complete the FISMA tab in SITR, which includes whether the information technology system is accredited through the DoD Information Assurance Certification and Accreditation Process or the Risk Management Framework.

*Table 1. Number of Information Technology Systems in SITR as of March 24, 2017 (cont'd)*

Component	Number of Systems in SITR
Army	3
U.S. Northern Command/North American Aerospace Defense Command	3
Air Force	1
Navy	1
Joint Staff	1
National Security Agency	1
Other DoD Components	0
<b>Total</b>	<b>199</b>

Source: SITR, as of March 2017.

## 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.<sup>9</sup> We identified internal control weaknesses related to the DoD CIO oversight of the information technology system information reported in SITR. We will provide a copy of the report to the senior official responsible for internal controls in the offices of the DoD and Component CIOs.

<sup>9</sup> DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

## Finding A

### DoD Components Did Not Report Accurate and Complete Data in SITR

DoD Components did not report accurate and complete information technology system data in SITR for 31 of the 32 information technology systems in our nonstatistical sample. Specifically:

- 21 information technology systems had inaccurate data in the core fields,
- 24 information technology systems had inaccurate data in the FISMA data fields,
- 11 information technology systems had incomplete data in the E-Authentication fields, and
- 4 information technology systems were incorrectly reported in SITR.<sup>10</sup>

DoD Components did not report accurate and complete information technology systems data in SITR because the DoD CIO did not:

- have a process to notify information technology system users of inaccurate SITR data,
- require SITR training for DoD Component personnel, or
- hold Component CIOs accountable for ensuring the accuracy and completeness of data reported in SITR.

As a result, the DoD cannot rely on SITR data. Unless data quality is improved, the DoD may not be able to effectively plan for continued operations of mission-critical or mission-essential information technology systems, use SITR for decision making as intended, which can affect stovepiped Component databases, mapping annual updates of the Business Enterprise Architecture, and making resource decisions; and the DoD may not be able to support its statutory compliance reporting designed to improve critical cybersecurity infrastructure.

<sup>10</sup> See page 2 of this report for more information about the core data fields.

## SITR Data Were Not Accurate and Complete

DoD Components did not report accurate and complete data in SITR for 31 of the 32 information technology systems in our nonstatistical sample. The 2007 and 2008 DITPR and SITR DoD CIO guidance states that DoD Components are responsible for the accuracy of all data entered into SITR.<sup>11</sup> To determine whether SITR data were accurate and complete, we met with the information technology system users to confirm information technology system data entered in SITR; we also reviewed supporting documentation related to the core, E-Authentication, and FISMA data fields. Based on the user-supplied information, supporting documentation, and our analysis, we identified information technology systems that had inaccurate core and FISMA data, incomplete E-Authentication data, and that were incorrectly included in SITR.

### *Inaccurate Core Data*

DoD Components reported inaccurate core data for 21 of 32 information technology systems. The 2007 and 2008 DITPR and SITR DoD CIO guidance states that the core data fields include the system name, system acronym, system component, system description, mission criticality, type of national security system, and whether the system interfaces with other systems. We reviewed the data in the core data fields and identified inaccuracies in the mission criticality and interfaces identified data fields. For example, for one information technology system we reviewed, USINDOPACOM personnel reported inaccurate information in the mission criticality data field. Specifically, SITR identified the system as a mission-essential system; however, the information system service description document identified the system as mission critical. For another information technology system we reviewed, USSOCOM personnel reported that the system did not have interfaces, but the system description documentation provided by the system user showed that the system had an interface with another information system. It is important for Components to correctly identify the criticality of an information system and whether it interfaces with another information system so Components can prioritize their response to a disruption in the operation of those information systems.

In addition, we could not verify the accuracy of all the core data fields for 9 of the 32 information technology systems. For example, for one information system, USSOCOM personnel could not provide documentation to support the core data entries for the system description, type of national security system, and interfaces.

---

<sup>11</sup> DoD CIO Memorandum, "DoD Information Technology (IT) Portfolio Repository (DITPR) and DoD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007 and 2008," September 6, 2007.

### ***Inaccurate FISMA Data***

DoD Components reported inaccurate FISMA data for 24 of the 32 information technology systems. The 2007 and 2008 DITPR and SITR DoD CIO guidance states that Components must enter FISMA data in SITR for all systems that require certification and accreditation. However, the May 2018 DITPR DoD CIO guidance states that the DoD CIO's goal is to remove the FISMA tab from DITPR and SITR in FY 2018. We reviewed the accuracy of 15 FISMA data fields for each system, and identified inaccuracies in the data fields for the mission assurance category, confidentiality level, system accreditation, security control test date, date annual security review, contingency plan, and contingency test. For example, one information technology system had inaccurate FISMA data in 6 of the 15 FISMA data elements included in SITR. Specifically, the system accreditation date, accreditation expiration, security control test date, date annual security review, contingency plan, and contingency test data fields were incorrect. One of the USINDOPACOM information technology systems had inaccurate data in 2 of the 15 FISMA data elements. Specifically, USINDOPACOM personnel entered incorrect information for the mission assurance category and confidentiality level data fields. It is important for Components to correctly identify the mission assurance category and confidentiality level of an information system so Components can ensure those systems are protected with the appropriate level of information assurance measures based on the sensitivity level of the information contained in the system.

In addition, we could not verify the accuracy of all the FISMA data fields for 25 of the 32 information technology systems. For example, for one information system, USSOCOM personnel could not provide documentation to support the FISMA data entries in SITR for the mission assurance category, security control test, date annual security review, and contingency test fields.

### ***Incomplete E-Authentication Data***

DoD Components did not report complete E-Authentication data in SITR for 11 of the 32 information technology systems. According to the 2007 and 2008 DITPR and SITR DoD CIO guidance, the E-Authentication initiative enables access to government systems in a secure, trusted environment, which enables secure Federal electronic business procedures. The Components are required to complete the browser-based, external-facing, and end-user authentication required E-Authentication data fields for all their systems. Accurate information is required to ensure adequate controls are in place for all systems.

In addition, we could not verify the accuracy of all the E-Authentication data fields for 9 of the 32 information technology systems. For example, for one information system, USSOCOM personnel could not provide documentation to support the

E-Authentication data entries for the browser-based and end-user authentication required fields. It is important for Components to complete the required E-Authentication data fields to ensure the Components have adequate controls in place for all systems.

### ***Incorrectly Reported Information Technology Systems***

DoD Components erroneously reported information technology systems in SITR for 4 of the 32 information technology systems we reviewed. The 2007 and 2008 DITPR and SITR DoD CIO guidance states that the Component responsible for obtaining the authorization to operate an information technology system is required to report the system in SITR. However, we determined that USINDOPACOM personnel incorrectly reported four information technology systems in SITR that another Component had obtained the authorization to operate. Specifically, one system had an authorization to operate from the National Security Agency, and an Air Force program office was responsible for authorizing and reporting another system. According to USINDOPACOM officials, the responsibility for authorizing and reporting one system was transferred from USINDOPACOM to the Defense Prisoner of War/Mission in Action Accounting Agency. In addition, USINDOPACOM officials stated that one system they reported incorrectly consolidated USINDOPACOM's nuclear command and control systems when USINDOPACOM officials should have reported them separately. USINDOPACOM personnel stated that they included the systems because they used SITR to maintain a historical record of all information technology systems connected to the USINDOPACOM network, regardless of ownership. However, as of May 2018, USINDOPACOM officials had removed the four systems they erroneously reported in SITR. As of June 2018, the systems had not been added back into SITR; however, the Component required to report the systems could have added the systems to a different information technology system repository.

### **DoD CIO Did Not Properly Manage SITR Data Quality**

DoD Components did not report accurate or complete information technology system data in SITR because the DoD CIO did not have a process to notify the information technology system users of inaccurate SITR data, did not require DoD Component personnel to take SITR training, and did not hold Component CIOs accountable for ensuring the accuracy and completeness of data reported in SITR.

### ***DoD CIO Had No Process to Notify Users of Inaccurate SITR Data***

DoD CIO officials did not have a process to notify information technology system users of inaccurate SITR data. The volume of errors that we identified support having an oversight and notification process in place to ensure the data in

SITR are correct. In May 2017, the DoD CIO recommended that USINDOPACOM officials review their SITR data for accuracy; however, the recommendation was made only after the DoD CIO was notified that our sample included USINDOPACOM. Although USINDOPACOM took corrective action in response to the recommendation, the corrective action did not address all problems with the data. Therefore, the DoD CIO should establish a process to notify the information technology system users of inaccurate data in SITR, give deadlines for corrections, and regularly follow up with DoD Components to ensure resolution.

### ***SITR Training Was Not Required***

The DoD CIO did not offer SITR training and neither did USSOCOM nor USINDOPACOM. The 21 information technology systems with inaccurate core data and the 26 information technology systems with inaccurate FISMA data that we identified clearly indicate that SITR training is necessary; therefore, the DoD CIO should require SITR training for all SITR and information technology system users to increase awareness of SITR's purpose, statutory requirements, and the importance of reporting accurate and complete data in SITR.

### ***No Accountability for Data Quality***

The DoD CIO did not hold DoD Component CIOs accountable for ensuring the accuracy and completeness of data reported in SITR. The DoD CIO issued a memorandum on July 14, 2017, that states the DoD CIO will send the Component CIOs a report identifying specific records and fields with questionable and missing data and the Component CIOs had 60 days from the date of the memorandum to correct the data in SITR.<sup>12</sup> The 2007 and 2008 DITPR and SITR DoD CIO guidance required DoD Component CIOs to certify, in writing, that all information technology system information reported in DITPR and SITR was accurate and complete. However, the DoD CIO issued a memorandum in 2009 that canceled the requirements for the DoD Component CIOs to certify the accuracy of DITPR and SITR. According to report number DODIG-2017-082, "a DoD CIO official stated that the certification requirement was canceled because DoD Components were knowingly submitting inaccurate certification documents just to comply with the 2007 and 2008 DITPR and SITR DoD CIO guidance." However, Federal law and DoD guidance state that the DoD CIO:

- is responsible for the DoD information enterprise, which includes SITR; and
- in performance of his or her duties assigned under Federal law, will ensure DoD Component CIOs comply with DoD policy.<sup>13</sup>

<sup>12</sup> DoD CIO Memorandum, "Registration of Information Technology Systems in Department of Defense Information Technology Portfolio Repository," July 14, 2017.

<sup>13</sup> 10 U.S.C. § 2223 (2011); 40 U.S.C. § 11315 (2012); and DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014.

To properly manage SITR data quality, the DoD CIO must hold DoD Component CIOs accountable for managing and ensuring the accuracy of information technology system data they report in SITR. Therefore, the DoD CIO should establish a process that holds DoD Component CIOs accountable for the accuracy and completeness of the data reported.

## SITR Data are Unreliable

The DoD cannot rely on the information technology system data in SITR for reporting requirements, as intended. Unless SITR data quality is improved, the DoD cannot effectively plan for the continued operations of mission-critical and mission-essential information technology systems, use SITR for decision making as intended, which can affect stovepiped Component databases, mapping annual updates for the Business Enterprise Architecture, and making resource decisions; and the DoD may not be able to support its statutory compliance reporting designed to improve critical cybersecurity infrastructure.

Federal law and DoD guidance require the DoD CIO to maintain a consolidated inventory of mission-critical and mission-essential information technology systems, to identify interfaces between those systems and other information systems, and develop and maintain contingency plans. The inaccurate and incomplete information technology system data in SITR limits the DoD's ability to plan for information technology system disruptions. Specifically, the DoD did not accurately identify whether information technology systems interfaced with other information technology systems. Therefore, the DoD may not be able to plan and respond to information technology disruptions.

## Recommendations

### ***Recommendation A.1***

**We recommend that the DoD Chief Information Officer:**

- a. Establish a process to notify the information technology system users of data inaccuracies in the SECRET Internet Protocol Router Network Information Technology Registry, give deadlines for corrections, and regularly follow up with DoD Components to ensure resolution.**
- b. Require SECRET Internet Protocol Router Network Information Technology Registry training for all SECRET Internet Protocol Router Network Information Technology Registry users and information technology system users to increase awareness of the SECRET Internet Protocol Router Network Information Technology Registry's purpose, statutory requirements, and the importance of reporting accurate and complete data.**

- c. **Establish a process that holds DoD Component Chief Information Officers accountable for the accuracy and completeness of information technology system data in the SECRET Internet Protocol Router Network Information Technology Registry.**

## **Management Actions Taken to Ensure Accurate and Complete Data in SITR**

On July 14, 2017, the DoD CIO issued a memorandum that implements a quarterly review process for SITR. Specifically, DoD Component CIOs are required to ensure their information technology systems are registered in DITPR or SITR and that the data the users enter is accurate and complete. The memorandum also states that the DoD CIO will send the Component CIOs a report identifying specific records and fields with questionable and missing data. Component CIOs had 60 days from the date of the memorandum to correct the data. Additionally, in January 2018 the DoD CIO initiated a training program for all SITR users. Available on the SITR website, the training defines the data that users are required to report in SITR and the importance of reporting accurate and complete data in SITR. In her comments to the draft report, the Principal Deputy CIO stated that the recommendations should be completed by the second quarter, FY 2020. Therefore, the recommendations are resolved but remain open.

## Finding B

### The DoD Maintains Similar Information Technology System Data in Multiple Repositories

The DoD maintains similar information technology system data in multiple repositories, including SITR, DITPR, the Enterprise Mission Assurance Support Service (eMASS), Xacta, and Archer. The eMASS, Xacta, and Archer repositories are cybersecurity management tools that are used to maintain the Risk Management Framework (RMF) documentation needed to authorize information technology systems to operate on DoD networks. Although the DoD uses the repositories to meet different requirements, the DoD has an opportunity for cost savings and efficiencies if it identifies a single enterprise solution to maintain RMF documentation that can also be used to respond to statutory requirements such as FISMA.

As of September 2017, DoD Components had spent approximately \$10 million for Xacta and Archer, systems that duplicate eMASS functionality (the Defense Information Systems Agency provides eMASS at no charge to DoD Components). In addition, SITR and DITPR require input of information that has already been entered into eMASS, Xacta, and Archer. On March 26, 2018, the Secretary of Defense issued a memorandum, “Be Peerless Stewards of Taxpayers’ Dollars,” which requested a commitment from all the DoD to exercise financial accountability on every expenditure. Minimizing duplicative information technology repositories in favor of an enterprise RMF documentation solution is potentially a step towards meeting that commitment.

### Risk Management Framework

The RMF was developed to establish a unified information security framework for the Federal Government. The RMF provides a structured yet flexible approach for managing organizational risk resulting from the use of information technology systems. Once an agency establishes baseline security controls for its information technology systems, those controls can be tailored and supplemented for specific systems based on the organization’s assessment of risk. Federal RMF guidance is contained in the National Institute of Standards and Technology Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems,” February 2010.<sup>14</sup> The Special Publication 800-37 details a six-step process for implementing RMF that can be applied to new and legacy

<sup>14</sup> Includes updates as of June 5, 2014.

information systems throughout a system's life cycle. DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, Incorporating Change 2, July 28, 2017, establishes the RMF as DoD's process for managing the life cycle cybersecurity risk to DoD information systems and contains the same six-step process detailed in the Special Publication for implementing RMF.

DoD Instruction 8510.01, states that an authorization to operate an information system cannot be made without completing the security authorization documentation and posting it in eMASS or using other RMF repositories. The Defense Information Systems Agency developed eMASS as a means to maintain required RMF documentation for DoD information technology systems. Instead of using eMASS, USSOCOM and the Air Force use Xacta and USINDOPACOM and the Marine Corps use Archer, to maintain their respective RMF documentation.

### ***eMASS***

eMASS is the Government-off-the-shelf web-based solution that maintains the documents needed to comply with RMF requirements.<sup>15</sup> eMASS contains documentation for over 18,000 information technology systems for more than 35 DoD Components. eMASS stores user information technology system inventory and system data, which Components report through the Enterprise Reporting Service. The Enterprise Reporting Service is a standalone web application that is the enterprise-reporting component of eMASS and contains a module for generating FISMA reports. DoD Components can obtain eMASS from the Defense Information Systems Agency for no cost.<sup>16</sup>

### ***Xacta***

USSOCOM and the Air Force use Xacta to maintain the RMF documentation needed to obtain an authorization to operate for their information systems and to maintain FISMA data. In September 2017, the Air Force awarded a contract, valued at \$6.2 million, to procure Xacta for 12 months to support Air Force enterprise risk management. The contract deliverables include software, training, support services, and an annual license. The Air Force Xacta contract includes a phase-based implementation strategy to use Xacta to maintain the required RMF assessment and authorization documents. Xacta also contains information technology system inventory and data, which supports FISMA reporting requirements. A USSOCOM official stated that they purchased Xacta in 2014 because eMASS did not have the capability of supporting top secret and special access program information.

<sup>15</sup> eMASS is jointly sponsored by the DoD CIO and the Defense Information Systems Agency.

<sup>16</sup> In addition, DoD Components have the option to add and pay for enhanced capabilities for their instance of eMASS.

## Archer

USINDOPACOM and the Marine Corps use the commercial RMF tool, Archer, to maintain the RMF documentation needed to obtain an authorization to operate for their information systems (the Marine Corps refers to Archer as the Marine Corps Compliance and Authorization Support Tool [MCCAST]). Archer also contains information technology system inventory and data, which supports FISMA reporting requirements. A USINDOPACOM official stated that USINDOPACOM uses Archer instead of eMASS because the functionality of Archer meets its business needs. Specifically, the USINDOPACOM official stated that USINDOPACOM uses Archer to support investment and budgeting decisions in addition to maintaining RMF documentation. The USINDOPACOM Authorizing Official Representative stated that Archer has a base cost of approximately \$100,000, and the assessment and authorization module costs approximately \$40,000. The Marine Corps Chief of the Cyber Security Division stated that MCCAST cost approximately \$3 million for licensing and labor in FY 2015.

## The DoD Maintains Similar Information Technology System Data in Multiple Repositories

The DoD maintains similar information technology system data in multiple repositories including SITR, DITPR, eMASS, Xacta, and Archer. We reviewed the data fields in SITR, DITPR, eMASS, Xacta, and Archer and determined that they contain the same types of information technology system data. For example, they all contain the mission assurance category, confidentiality level, security review date, security control test, contingency plan required, contingency plan tested, accreditation status, accreditation date, and accreditation expiration data fields which are required for FISMA. Table 2 identifies the duplicate data fields in SITR, DITPR, eMASS, Xacta and Archer as of March 24, 2017.

Table 2. Duplicate Data Fields in Repositories as of March 24, 2017

Data	SITR	DITPR	eMASS	Xacta	Archer/ MCCAST
Component	X	X	X	X	X
System Name	X	X	X	X	X
Record Type/Type of System	X	X	X	X	X
System Acronym	X	X	X	X	X
Mission Assurance Category	X	X	X	X	X
Confidentiality Level	X	X	X	X	X

Table 2. Duplicate Data Fields in Repositories as of March 24, 2017 (cont'd)

Data	SITR	DITPR	eMASS	Xacta	Archer/ MCCAST
National Security System	X	X	X	X	X
Security Review Date	X	X	X	X	X
Security Control Test	X	X	X	X	X
Contingency Plan Required	X	X	X	X	X
Contingency Plan Tested	X	X	X	X	X
Accreditation Status	X	X	X	X	X
Accreditation Date	X	X	X	X	X
Accreditation Expiration	X	X	X	X	X

Source: The DoD OIG.

## DoD Chief Information Officer Can Gain Efficiencies in Reporting Information Technology System Data

Although the DoD uses SITR, DITPR, eMASS, Xacta, and Archer to meet different requirements, the DoD may have an opportunity for cost savings and efficiencies if it identifies a single enterprise solution for RMF that can also be used to respond to statutory requirements such as FISMA. Furthermore, to support an authorization to operate, the DoD Components used the DoD-recommended tool eMASS or commercial RMF tools, Xacta and Archer, to maintain assessment and authorization RMF documentation for their information technology systems. In addition, SITR and DITPR require the input of information that the DoD has already entered into eMASS, Xacta, and Archer, which is a duplication of effort. The DoD CIO has not completed an evaluation to determine what efficiencies would result from reducing multiple information technology system repositories used to capture similar information technology system data. Identifying efficiencies aligns with the Secretary of Defense's February 2017 memorandum, which directs the DoD to continue working to find efficiencies in core business functions, such as cyber and information technology management.<sup>17</sup> Therefore, the DoD CIO should conduct a study to determine the most effective process and information technology repository for maintaining and reporting information technology data and eliminate any duplicate processes associated with the information technology repositories.

<sup>17</sup> Secretary of Defense Memorandum, "Establishment of Cross-Functional Teams to Address Improved Mission Effectiveness and Efficiencies in the DoD," February 17, 2017.

USSOCOM, USINDOPACOM, and the Air Force do not use eMASS because the DoD CIO has not mandated the use of eMASS, and because, as of March 2018, eMASS does not have the capability to maintain top secret information technology system data. The Defense Information Systems Agency eMASS Program Manager stated that eMASS will have the capability to maintain top secret and special access program data by the end of 2018.

The DoD CIO has not required DoD Components to conduct and submit a business case analysis before making the determination on whether to use a commercial RMF tool, rather than using eMASS.<sup>18</sup> The DoD CIO should require DoD Components to conduct and submit a business case analysis before selecting a commercial RMF tool, rather than using eMASS. In addition, the DoD CIO should establish a process to evaluate the DoD Components' business case analysis before selecting a commercial RMF tool rather than eMASS. Furthermore, the DoD CIO should require all DoD Components to use eMASS when the DoD develops the capability for eMASS to maintain top secret information technology system data.

## **The DoD Can Potentially Use Information Technology Repositories More Efficiently**

On March 26, 2018, the Secretary of Defense issued a memorandum, "Be Peerless Stewards of Taxpayers' Dollars." The memorandum requested a commitment from all of the DoD to exercise financial accountability on every expenditure. Minimizing duplicative information technology repositories in favor of an enterprise RMF solution is potentially a step towards meeting that commitment. When DoD Components continue to maintain multiple repositories with duplicate functionality instead of using the existing enterprise solution, eMASS, it goes against practicing a culture of responsible financial stewardship. Specifically, as of September 2017, DoD Components have spent approximately \$10 million for Xacta and Archer commercial RMF tools that duplicate eMASS functionality. The Defense Information Systems Agency provides eMASS at no charge to DoD Components. Therefore, when DoD Components use the DoD-recommended tool, eMASS, costs associated with using commercial RMF tools are eliminated, and it reduces the potential of wasting resources.

---

<sup>18</sup> According to the Defense Acquisition University, a business case analysis aids decision making by identifying and comparing alternatives by examining the mission and business impacts. It is a documented objective value analysis that explores costs, benefits, and risks.

## Recommendations, Management Comments, and Our Response

### **Recommendation B.1**

We recommend that the DoD Chief Information Officer:

- a. **Conduct a study to determine the most effective process and information technology repository for maintaining and reporting information technology data and eliminate any duplicate processes associated with the information technology repositories.**

#### *Principal Deputy Chief Information Officer Comments*

The Principal Deputy CIO, responding for the DoD CIO, disagreed but stated that the office of the DoD CIO has initiated a reform project to account for and reduce information technology repositories, optimize cost, and improve data efficiency. She also stated that through the process a core set of reference management framework tools will be established to support Component and enterprise requirements.

#### *Our Response*

Comments from the Principal Deputy CIO addressed all specifics of the recommendation; therefore, the recommendation is resolved. We will close the recommendation once we verify that an effective process has been identified and that duplicate processes have been eliminated.

- b. **Require DoD Components to conduct and submit a business case analysis to the DoD Chief Information Officer before selecting or renewing the use of a commercial Risk Management Framework accreditation and authorization tool, rather than using the Enterprise Mission Assurance Support Service.**
- c. **Develop a process to evaluate and approve DoD Components' business case analysis for the use of a commercial Risk Management Framework accreditation and authorization tool, rather than using the Enterprise Mission Assurance Support Service.**

#### *Principal Deputy Chief Information Officer Comments*

The Principal Deputy CIO, responding for the DoD CIO, disagreed stating that these recommendations do not consider guidance already in place regarding the use of business case analysis to inform investment decisions.

### *Our Response*

Comments from the Principal Deputy CIO partially addressed the recommendations concerning the DoD Components' use of business case analysis before selecting a commercial RMF tool; therefore, the recommendations are unresolved. We acknowledge that guidance is in place regarding the use of business case analysis; however, during our audit the DoD Components could not provide a business case analysis to justify their selection of a commercial RMF tool rather than the DoD-recommended tool eMASS. Therefore, the DoD CIO should provide additional comments specifying how he will ensure that DoD Components conduct and submit a business case analysis before they select or renew the use of a commercial RMF accreditation and authorization tool rather than eMASS. The DoD CIO should also specify a process to evaluate and approve the business case analyses.

- d. Require all DoD Components to use the Enterprise Mission Assurance Support Service when the DoD develops the capability for the Enterprise Mission Assurance Support Service to maintain top secret information technology system data.**

### *Principal Deputy Chief Information Officer Comments*

The Principal Deputy CIO, responding for the DoD CIO disagreed with the recommendation.

### *Our Response*

Comments from the Principal Deputy CIO did not address the specifics of the recommendation; therefore, the recommendation is unresolved. The DoD CIO should provide additional comments specifying how the DoD Components will be required to use eMASS when the DoD develops the capability for eMASS to maintain top secret information technology system data.

## Appendix

---

### Scope and Methodology

We conducted this performance audit from April 2017 through July 2018 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

### *Universe and Sample Selection*

We obtained a copy of the SITR core data spreadsheet on March 24, 2017, that identified 199 information technology systems from 13 Combatant Commands and Defense agencies. Because USINDOPACOM and USSOCOM had the most information technology systems in SITR, with 96 and 37 information technology systems, respectively, we focused on information technology systems within those commands. We nonstatistically selected 15 information technology systems from USINDOPACOM, and 17 information technology systems from USSOCOM by randomly selecting a sample from the SITR core data spreadsheet.

### *Information Technology System Data Analyses*

To determine the accuracy of the core, FISMA, and E-Authentication data entries in SITR we reviewed information technology system documentation and compared it to the data entries reported for the information technology system in SITR. For the USSOCOM information technology systems in our sample, we visited USSOCOM headquarters in Tampa, Florida, to interview the information technology systems' users about the process of entering information for their information technology systems into SITR.

During the audit, we determined that USSOCOM and USINDOPACOM used other information technology systems that had similar data fields as SITR. The repositories, eMASS, Xacta, and Archer, were designed to ensure the DoD Components complied with RMF requirements. To learn more about those information technology systems, we interviewed personnel at the Defense Information Systems Agency to discuss eMASS, personnel at USSOCOM to discuss Xacta, and personnel at USINDOPACOM to discuss Archer. We obtained documentation from the DoD Components on the cost of the Xacta and Archer commercial RMF tools and requested information to support why eMASS could not meet their business needs.

## **Criteria Reviewed**

We reviewed the following regulations and guidance to determine whether DoD Components reported accurate and complete data in SITR:

- 10 U.S.C. § 2223, “Information Technology: Additional Responsibilities of Chief Information Officers,” October 1, 1998, Updated on January 7, 2011;
- Public Law 113-283, “Federal Information Security Modernization Act of 2014,” December 18, 2014; and
- DoD CIO Memorandum, “Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007-2008,” September 6, 2007.

We reviewed the following regulations and guidance to determine whether DoD Components are required to use a specific tool for the RMF process:

- National Institute of Standards and Technology Special Publication 800-37, “Guide for Applying the Risk Management Framework to Federal Information Systems,” February 2010, Includes Updates as of June 5, 2014; and
- DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014, Incorporating Change 2, July 28, 2017.

## **Use of Computer-Processed Data**

We used computer-processed data from DITPR and eMASS to perform this audit. We queried DITPR to determine whether it contained data fields that were similar to SITR, eMASS, Xacta, and Archer. In addition, we reviewed information technology system documentation stored in eMASS and an eMASS data field spreadsheet to determine whether the data fields in eMASS were similar to DITPR, SITR, Xacta, and Archer. We did not test the accuracy and reliability of the data we reviewed from DITPR and eMASS because we reviewed the data from the repositories only to determine whether the DoD could gain efficiencies by reducing the number of systems used to store similar data.

## **Prior Coverage**

During the last 5 years, the DoD Office of Inspector General (DoD OIG) issued one report on the accuracy and completeness of repositories that store data of classified information technology systems. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/reports.html/>.

**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 identified that DoD Components did not report complete and accurate information technology system data in DITPR for 19 of the 31 information technology systems in the nonstatistical sample. The report concluded that the DoD cannot rely on the accuracy and completeness of the data in DITPR.

# Management Comments

## DoD Chief Information Officer



CHIEF INFORMATION OFFICER

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

SEP 04 2018

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Draft Report "DoD Information Technology System Repositories" (Project No. D2017-D000RD-0134.000)

The Department of Defense Chief Information Officer (DoD CIO) conducted a review of the DoD IG Draft Report, "DoD Information Technology System Repositories" (Project No. D2017-D000RD-0134.000), and our response is attached.

DoD CIO concurs with Finding A recommendations. As mentioned in this report, recommended steps have been initiated to account for the completeness and accuracy of SITR data. We plan to complete these recommendations by second quarter of fiscal year 2020.

DoD CIO non-concurs with Finding B recommendations. These recommendations do not consider guidance already in place regarding use of business case analysis to inform investment decisions. This office has initiated a reform project to establish a better defined process to account for and reduce information technology management repositories, optimize cost, and to improve data efficiency. It is planned that through this process, a core set of reference management framework tools will be established to support Component and enterprise requirements.

The point of contact for this matter is [REDACTED]

*Essy B. Miller*  
Essy B. Miller  
Principal Deputy

## Acronyms and Abbreviations

---

<b>CIO</b>	Chief Information Officer
<b>DITPR</b>	DoD Information Technology Portfolio Repository
<b>eMASS</b>	Enterprise Mission Assurance Support Service
<b>FISMA</b>	Federal Information Security Modernization Act
<b>MCCAST</b>	Marine Corps Compliance and Authorization Support Tool
<b>RMF</b>	Risk Management Framework
<b>SIPRNET</b>	SECRET Internet Protocol Router Network
<b>SITR</b>	SECRET Internet Protocol Router Network Information Technology Registry
<b>U.S.C.</b>	United States Code
<b>USINDOPACOM</b>	United States Indo-Pacific Command
<b>USSOCOM</b>	United States Special Operations 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/](http://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/](http://www.dodig.mil/Mailing-Lists/)

**Twitter**

[www.twitter.com/DoD\\_IG](http://www.twitter.com/DoD_IG)

**DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
Defense Hotline 1.800.424.9098

