



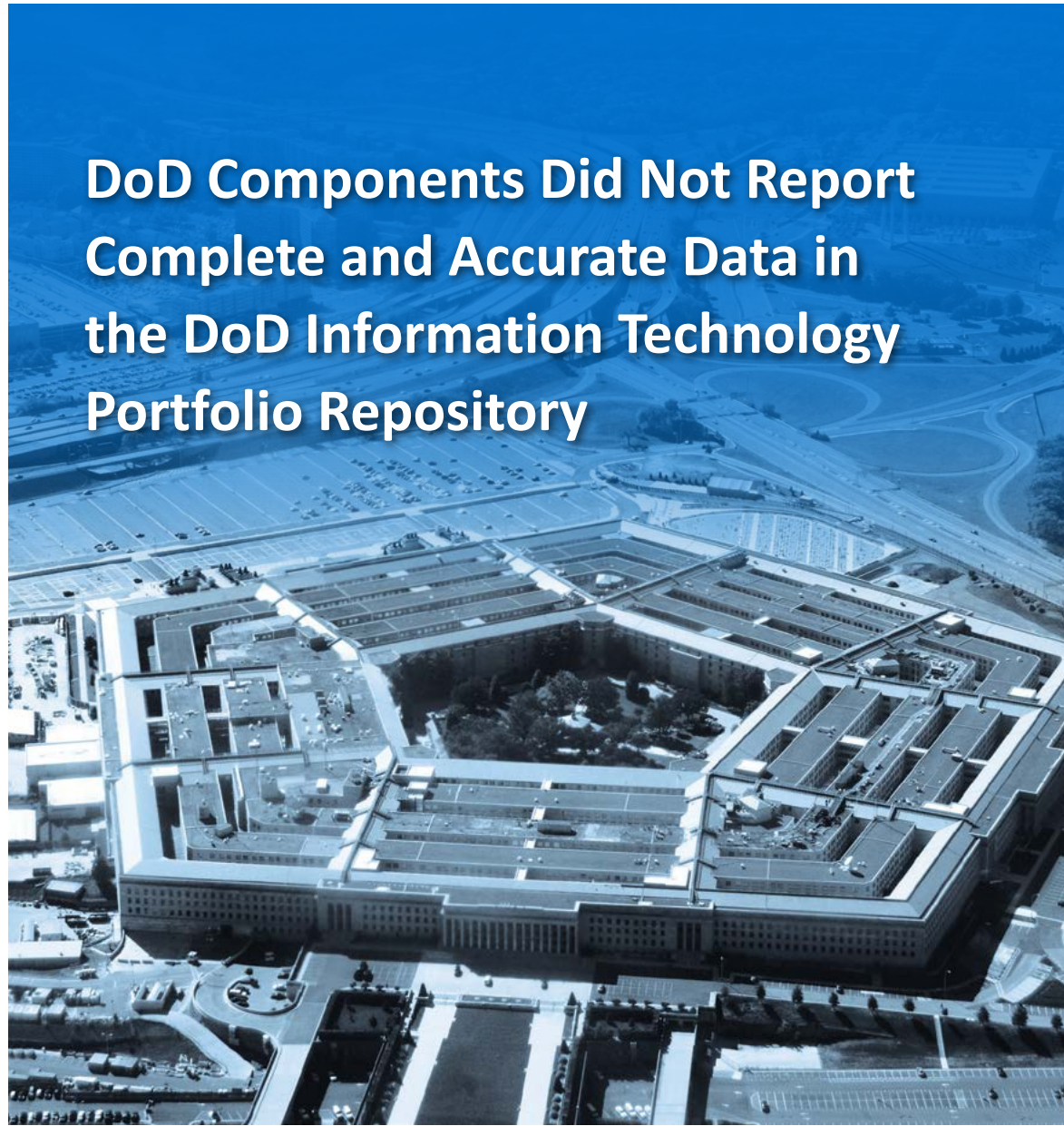
INSPECTOR GENERAL

U.S. Department of Defense

MAY 10, 2017



DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.



Results in Brief

DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository

May 10, 2017

Objective

We determined whether DoD Components reported complete and accurate information technology (IT) systems data into the DoD Information Technology Portfolio Repository (DITPR).

Background

DoD guidance states that DITPR is the authoritative unclassified inventory of the DoD's mission-critical and mission-essential IT systems. Mission-critical IT systems are necessary to continue warfighter operations and direct mission support of warfighter operations, while mission-essential IT systems are basic and necessary to accomplish an organization's mission. DITPR contains information required for analyzing DoD inventory, portfolios, and capabilities. As of April 2016, DITPR contained system information for 6,169 individual IT systems across 47 DoD Components.

Finding

DoD Components did not report complete and accurate IT system data in DITPR for 19 of the 31 IT systems in our nonstatistical sample. Specifically:

- 4 systems had incorrect mission assurance categories;¹
- 3 systems should not have been reported in DITPR as active IT systems;

¹ A mission assurance category is assigned to systems based on the importance of the system to the achievement of DoD goals and objectives. Level I systems are vital to operational readiness or mission effectiveness, level II systems are important to operational readiness and effectiveness, and level III systems are necessary for the conduct of day-to-day business.

Finding (cont'd)

- 4 systems were incorrectly categorized as National Security Systems,² as defined by the National Institute of Standards and Technology; and
- 11 systems had an inaccurate number of interfacing systems.³ Interface is defined as a common boundary between independent systems or modules where interactions take place.

Additionally, through reviews of all 6,169 IT systems reported in DITPR as of April 20, 2016, we identified 2,992 IT systems with incomplete data. DoD Components did not report complete and accurate IT system data in DITPR because the DoD Chief Information Officer did not:

- hold Component Chief Information Officers accountable for ensuring the completeness and accuracy of IT system data in DITPR;
- ensure DoD Components corrected errors identified during periodic data reviews; or
- require adequate DITPR training for DoD Component personnel.

The DoD cannot rely on DITPR data and has spent at least \$30.8 million since 2004 to operate, maintain, and update a system that contains incomplete and inaccurate IT system data. Unless data quality is improved, the DoD cannot effectively plan for the continued operations of mission-critical and mission-essential IT systems, use DITPR for decision making as intended, or support statutory compliance reporting. For example, inaccurate and incomplete interfacing system information limits DoD's ability to plan for IT system disruptions. Because disruptions in one IT system can result in disruptions in interfacing systems, it is critical for contingency planning that interface data is

² National Security Systems are systems that involve (1) intelligence activities, (2) national security cryptologic activities, (3) command and control of military forces, or (4) equipment that is part of a weapon or weapon system; and systems that are (5) critical to the direct fulfillment of military or intelligence missions; or (6) classified by Executive Order or Act of Congress.

³ The total number of systems with errors –19– does not equal the sum of the errors –22– because three systems had more than one inaccuracy.



Results in Brief

DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository

Finding (cont'd)

accurate and complete. Unexpected disruption in the use of a mission-critical or mission-essential IT system could negatively impact warfighter operations or direct mission support for warfighter operations.

Recommendations

We recommend that the DoD Chief Information Officer:

- establish a process that holds DoD Component Chief Information Officers accountable for the completeness and accuracy of IT system data in DITPR;
- notify IT system owners of data deficiencies, give deadlines for corrections, and regularly follow up with DoD Components to ensure resolution; and
- require DITPR training for all DITPR users and IT system owners and add training content on DITPR's purpose, statutory requirements, and relationship to DoD feeder systems.

Management Comments and Our Response

The Acting Principal Deputy, DoD Chief Information Officer, commenting for the DoD Chief Information Officer, addressed all specifics of the recommendations to hold DoD Component Chief Information Officers accountable for the completeness and accuracy of DITPR data and to notify IT system owners of data deficiencies, provide deadlines for corrections, and regularly follow up with DoD Components to ensure resolution. Therefore, the recommendations are resolved and will be closed once we verify that a semiannual data quality review process is initiated and monthly data quality checks include the setting of deadlines and followup to ensure resolution of data deficiencies.

The Acting Principal Deputy, DoD Chief Information Officer, commenting for the DoD Chief Information Officer, partially addressed the recommendation to require DITPR training for all DITPR users and to add training content on DITPR's purpose, statutory requirements, and relationship to feeder systems. Therefore, the recommendation is unresolved. The DoD Chief Information Officer should provide comments to the final report specifying how he will require all DITPR users to complete the necessary training. We request that the DoD Chief Information Officer provide comments to the final report by June 9, 2017. Please see the Recommendations Table on the next page.

Recommendations Table

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

Please provide Management Comments by June 9, 2017.

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**

May 10, 2017

MEMORANDUM FOR DOD CHIEF INFORMATION OFFICER

**SUBJECT: DoD Components Did Not Report Complete and Accurate Data in the DoD
Information Technology Portfolio Repository (Report No. DODIG-2017-082)**

We are providing this report for review and comment. DoD Components did not report complete and accurate IT system data in DITPR. The DoD spent at least \$30.8 million to operate, maintain, and update DITPR; but incomplete and inaccurate IT system data make the information contained in DITPR unreliable. 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 Acting Principal Deputy, DoD Chief Information Officer, commenting on behalf of the DoD Chief Information Officer, addressed Recommendations 1.a and 1.b; therefore, the recommendations are resolved. Comments from the Acting Principal Deputy partially addressed Recommendation 1.c; therefore, the recommendation is unresolved. We request that the DoD Chief Information Officer provide additional comments on Recommendation 1.c, by June 9, 2017.

Please send a PDF file containing your comments to audrco@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 courtesies extended to the staff. Please direct questions to me at (703) 699-7331 (DSN 664-7331).

A handwritten signature in black ink, reading "Carol N. Gorman", is positioned above the printed name.

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations



Contents

Introduction

Objective	1
Background	1
Review of Internal Controls	4

Finding. DoD Components Did Not Report Complete and Accurate Data in DITPR

5

DoD Components Reported Inaccurate Data in DITPR	5
DITPR Database Deficiencies	9
DoD CIO Did Not Properly Manage DITPR Data Quality	11
DITPR Information is Unreliable	13
Management Comments on the Finding and Our Response	14
Recommendations, Management Comments and Our Response	16
Unsolicited Management Comments on the Recommendations and Our Response	17

Appendix

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

Management Comments

DoD Chief Information Office	22
Defense Information Systems Agency	25

Acronyms and Abbreviations

27

Introduction

Objective

Our audit objective was to determine whether DoD Components reported complete and accurate information technology (IT) systems⁴ data into the DoD Information Technology Portfolio Repository (DITPR). See the Appendix for a discussion of the scope and methodology and prior audit coverage.

Background

DoD guidance states that DITPR is the authoritative unclassified inventory⁵ of the DoD's mission-critical and mission-essential IT systems.⁶ DITPR is a web-based system that contains information on DoD IT systems, including system names, acronyms, descriptions, sponsoring Components, approval authority points of contact, life-cycle dates, and other information required for analyzing DoD inventory, portfolios, and capabilities. As of April 20, 2016, DITPR contained system information for 6,169 individual IT systems across 47 DoD Components.

The DoD uses DITPR data to meet a wide variety of internal and external reporting requirements, including regularly scheduled reports required by legislative or regulatory mandates, annual reports required by other Federal Departments, and ad hoc reports using data subsets. For example, the DoD CIO uses DITPR data to report quarterly and annual DoD Component IT system security metrics to the Office of Management and Budget. DITPR is also the data source for the reporting required to comply with the following.

- 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.⁷
- The Clinger-Cohen Act of 1996—requires DoD Component Chief Information Officers (CIOs) to assist in capital investment evaluations and decision making for all programs that acquire IT, including mission-critical and mission-essential systems.⁸

⁴ An IT system collects, processes, maintains, shares, disseminates, or disposes of information.

⁵ According to DoD officials, the unclassified DITPR includes systems that process classified information, provided that the information needed to register the system is unclassified and no classified information is disclosed.

⁶ A mission-critical IT system is a system whose loss would stop warfighter operations or direct mission support of warfighter operations. A mission-essential IT system is a system that is basic and necessary to accomplish an organization's mission.

⁷ Section 552a, title 5, United States Code (5 U.S.C. § 552a [2012]).

⁸ 40 U.S.C. § 1401 et seq. (1998).

- The E-Government Act of 2002—requires Privacy Impact Assessments (PIAs) to be completed and approved to ensure that personally identifiable information⁹ in electronic forms is collected, stored, protected, used, shared, and managed in a manner that protects privacy.¹⁰
- The Office of Management and Budget—requires that each Federal agency review new and existing electronic transactions to ensure that authentication¹¹ processes provide the appropriate level of assurance.¹²
- The Federal Information Security Modernization Act of 2014 (FISMA)—requires each Federal agency to evaluate and test the effectiveness of its information security programs.¹³

Roles and Responsibilities

To develop and maintain contingency plans for responding to the disruption in the operations of mission-critical information systems, section 2223, title 10, United States Code, 2014 (10 U.S.C. § 2223 [2014]), requires the DoD CIO to maintain a consolidated inventory of DoD mission-critical and mission-essential information systems and identify interfaces between those systems and other information systems.¹⁴ The DoD CIO is also required to:

- oversee the management of information resources to improve the integrity, quality, and utility of information for all those who use the information within and outside the DoD;
- ensure that the Military Department CIOs comply with 10 U.S.C. § 2223 (2014), which requires that IT systems meet DoD and Federal standards;¹⁵ and
- ensure that all DoD Component CIOs comply with DoD policy under the purview of the DoD CIO.¹⁶

The Department of the Navy Program Executive Office for Enterprise Information Systems manages DITPR for the DoD CIO. Component CIOs must ensure that IT systems within their Components are registered in DITPR. The DoD CIO and the Department of the Navy CIO hold monthly integrated process team (IPT) meetings with the Components during which DoD CIO representatives discuss the status of DITPR, data quality issues, technical and DITPR guidance updates, and other areas of concern.

⁹ Information about an individual that identifies, describes, or is unique to the individual.

¹⁰ Public Law 107-347.

¹¹ Authentication focuses on confirming a person's identity, based on their credentials.

¹² Office of Management and Budget Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," December 16, 2003.

¹³ 44 U.S.C. § 3551 et seq. (2014).

¹⁴ Independent systems interface when they interact across a common boundary.

¹⁵ These responsibilities include ensuring compliance with Government and DoD standards for IT and national security systems.

¹⁶ DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014.

DITPR Data Procedures

The Military Departments enter data into their respective IT inventory feeder systems that automatically upload the data into DITPR. The other DoD Components manually enter their IT system data directly into DITPR. Information entered into DITPR populates data elements that are grouped into the following data sets.¹⁷

- **Core-basic:** a single data set that provides general information for each reported IT system, including system name, description, Component, points of contact, and whether the IT system meets the definition of a National Security System (NSS),¹⁸ along with other general information.
- **Core-trigger:** seven data sets that identify whether a DoD Component must provide data elements for DITPR to use in compliance-specific data sets. For example, the FISMA core-trigger question asks whether the IT system requires DoD-approved IT security certification and accreditation. If the answer is yes, the system representative must complete 12 FISMA compliance-specific data elements.
- **Compliance-specific:** 13 data sets that support internal and external reporting requirements, including FISMA, PIA, Privacy Act, Public Key (PK) Infrastructure, E-Authentication requirements, and 10 U.S.C. § 2222 (2014). Four of these data sets are not contingent on answers to trigger questions because they apply to all IT systems.
- **Core-Warfighting Mission Area:** a single data set that provides the warfighting priorities of the Combatant Commanders and the Joint Chiefs of Staff.
- **System budget:** a single data set that provides the option to track budget information about entries across the Future Years Defense Plan.

To determine whether DITPR data were complete, we analyzed core-trigger and compliance-specific data sets because of their impact on external reporting. To determine whether DITPR data were accurate, we tested a nonstatistical sample of IT systems in DITPR.

¹⁷ A data set is a collection of data records for computer processing.

¹⁸ An NSS is defined by Federal law at 44 U.S.C. § 3552 (2014) as any information system, including telecommunications systems, used or operated that involves intelligence activities, national security cryptologic activities, or command and control of military forces. This includes equipment that is an integral part of a weapon or weapons system; with some exceptions, is critical to the fulfillment of military or intelligence missions; or is protected by procedures authorized to be kept classified in the interest of national defense or foreign policy.

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.¹⁹ We identified internal control weaknesses related to DoD CIO oversight of the system information reported in DITPR. Specifically, the DoD CIO did not ensure that DoD Components reported accurate mission assurance category (MAC) levels, systems status, NSS categorization, and interfacing system information. Additionally, we identified 2,992 IT systems with incomplete data in DITPR. We will provide a copy of the final report to the senior official responsible for internal controls in the offices of the DoD and Component CIOs.

¹⁹ DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

DoD Components Did Not Report Complete and Accurate Data in DITPR

DoD Components did not report complete and accurate IT system data in DITPR for 19 of the 31 IT systems in our nonstatistical sample. Specifically:

- 4 systems had incorrect MAC levels;
- 3 systems should not have been reported in DITPR as active IT systems;
- 4 systems were incorrectly categorized as NSS; and
- 11 systems had an inaccurate number of interfacing systems.²⁰

Additionally, through reviews of all 6,169 IT systems reported in DITPR as of April 20, 2016, we identified 2,992 IT systems with incomplete data. DoD Components did not report complete and accurate IT system data in DITPR because the DoD CIO did not:

- hold Component CIOs accountable for ensuring the completeness and accuracy of data reported in DITPR;
- ensure DoD Components corrected errors identified during periodic data reviews; or
- require adequate DITPR training for DoD Component personnel.

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

DoD Components Reported Inaccurate Data in DITPR

DoD Components reported inaccurate data in DITPR for 19 of the 31 IT systems included in our nonstatistical sample. See the Appendix for information on our nonstatistical sample and our methodology. DITPR guidance states that DoD Components “own” the information in DITPR and are responsible for the accuracy

²⁰ The total number of systems with errors does not equal the sum of the errors because three systems had more than one inaccuracy.

of all data entered.²¹ To determine whether DoD Components accurately reported IT system data in DITPR, we reviewed DITPR system information and developed standard questions, based on Federal and DoD requirements, that we asked system representatives. We also met with IT system representatives to obtain confirmation of system information in DITPR, as well as supporting documentation related to FISMA, PIA, Privacy Act, E-Authentication, and interfacing requirements. Based on Component answers to our questions and our analysis, we identified IT systems that had an inaccurate MAC, were erroneously included in DITPR, had an inaccurate NSS status, or had an inaccurate number of interfacing systems. See the table for a summary, by DoD Component, of the number of sample items reviewed and inaccuracies identified.

Table. Inaccurate Data Reported From Nonstatistical Sample of IT Systems

Component Reviewed*	Total Systems Reviewed	Incorrect Data Category				Total Systems With Incorrect Data
		MAC Status	Systems Erroneously Included In DITPR	NSS Status	Interfacing Systems	
Army	13	4	2	1	5	10
DISA	4	0	1	1	1	2
DLA	3	0	0	0	2	2
DON/USMC	3	0	0	0	0	0
OSD CIO	5	0	0	2	3	5
USTRANSCOM	3	0	0	0	0	0
Total	31	4**	3	4	11	19

* Defense Information Systems Agency (DISA), Defense Logistics Agency (DLA), Department of the Navy/United States Marine Corps (DON/USMC), Office of the Secretary of Defense (OSD), United States Transportation Command (USTRANSCOM).

** The Army downgraded the MAC level for one of these systems in DITPR after the April 2016 data was pulled.

Inaccurate MAC Levels

DoD Components inaccurately categorized the MAC level for 4 of the 31 IT systems. DITPR guidance requires DoD Components to report whether an IT system is a MAC I, MAC II, or MAC III level system. The MAC level reflects the importance of system information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission. Specifically, DoD guidance defines MAC levels as follows.

- MAC I systems handle information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of

²¹ "DoD IT Portfolio Repository (DITPR) and DoD SIPRNET IT Registry Guidance," 2007-2008, issued by the DoD CIO on September 6, 2007.

integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. MAC I systems require the most stringent protection measures.

- MAC II systems handle information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of system availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. MAC II systems require additional safeguards beyond best practices to ensure adequate assurance.
- MAC III systems handle information that is necessary for the conduct of day-to-day business, but does not materially affect the support of deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. MAC III systems require protective measures, techniques, or procedures generally commensurate with commercial best practices.²²

In DITPR, all 31 of the IT systems in our sample were reported by DoD Components as MAC I systems. To verify that the MAC level was correct, we spoke with the system representatives and analyzed supporting documentation. We verified that 27 of the systems were MAC I systems, but the other 4 were not. System representatives for the four IT systems stated that the systems were actually MAC II or MAC III systems. Specifically, the system representatives acknowledged that they had downgraded the four IT systems from MAC I, but had not updated DITPR to reflect the changes. According to system representatives, two of the sample IT systems were downgraded to MAC III in 2014, but as of January 2017, remained categorized as MAC I in DITPR.

Erroneously Included IT Systems

DoD Components erroneously included 3 of the 31 IT systems in DITPR. DITPR guidance requires DoD Components to request that retired or replaced IT systems be listed in DITPR as archived, which removes the IT systems from DITPR's active file. DITPR guidance also provides entry criteria and lists examples of the information that should and should not be included in DITPR. For example, enclaves²³ should be included in DITPR as separate IT systems but commercial off-the-shelf systems²⁴ should not.

²² DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004.

²³ An enclave is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy.

²⁴ Commercial off-the-shelf systems are systems that are ready-made and available for sale to the general public.

We determined that three of the systems in our sample did not meet the definition of a system, as defined by Federal law,²⁵ or were no longer an active system. One system was no longer an active system and had been replaced in 2014. Another system was not an enclave as reported in DITPR but instead was a data center²⁶ for IT systems controlled remotely by other DoD and Federal agencies. The remaining system was a commercial off-the-shelf product.

Incorrect National Security System Designation

DoD Components incorrectly designated 4 of the 31 IT systems as NSS. An NSS is defined by Federal law²⁷ as any information system, including telecommunications systems, used or operated that involves intelligence activities, national security cryptologic activities, command and control of military forces, equipment that is an integral part of a weapon or weapons system, is a system critical to the fulfillment of military or intelligence missions, or is protected by procedures authorized to be kept classified in the interest of national defense or foreign policy. National Institute of Standards and Technology guidance requires agencies to identify all NSS under their control.²⁸ DITPR guidance requires DoD Components to indicate in DITPR whether IT systems are NSS, and, if so, indicate the NSS classification criteria met. We compared the descriptions of our sample IT systems to the definition of an NSS and determined that three IT systems were incorrectly designated as NSS and a fourth IT system was a data center, not a system.

Inaccurate Number of Interfacing Systems

DoD Components inaccurately identified interfacing system information for 11 of the 31 IT systems. To develop and maintain contingency plans for responding to the disruption in the operations of mission-critical information systems, Federal law and DoD guidance require the DoD CIO to identify interfaces between mission-critical and mission-essential IT systems and other systems.²⁹ However, the DITPR guidance requires DoD Components to input only the number of interfacing systems for each IT system registered in DITPR. Providing only the number of systems does not provide sufficient information to identify the interfacing systems for contingency planning purposes. Additionally, according to a DoD CIO official, there is no clear definition of what constitutes an interfacing

²⁵ 44 U.S.C. § 3502 (2011) defines an information system as a set of resources organized to collect, process, maintain, share, disseminate, or dispose of information.

²⁶ A data center is a repository that houses computing facilities such as servers, routers, switches, and firewalls, as well as supporting components such as backup equipment, fire suppression facilities, and air conditioning.

²⁷ 44 U.S.C. § 3552 (2014).

²⁸ National Institute of Standards and Technology Special Publication 800-59, "Guideline for Identifying an Information System as a National Security System," August 2003.

²⁹ 10 U.S.C. § 2223 (2014); DoD Directive 5144.02.

system to help DoD Components identify interfaces. We reviewed DITPR reports, other supporting documentation, and interviewed the IT system owners to determine whether DoD Components accurately reported interface information. We determined that for 11 IT systems, DoD Components entered an inaccurate number of interfacing systems in DITPR. For example, DITPR indicated that a sample Army IT system had no interfacing systems, but the IT system's owner provided a list showing that it interfaced with eight other systems.

DITPR Database Deficiencies

Through data reviews for the 6,169 systems reported in the DITPR database as of April 20, 2016, we identified 2,992 IT systems with incomplete data.

Through data reviews for the 6,169 systems reported in the DITPR database as of April 20, 2016, we identified 2,992 IT systems with incomplete data. DITPR guidance states that DoD Components are responsible for the completeness of all data entered. To determine whether DoD Component IT system data in DITPR were complete, we reviewed the DITPR guidance list of core-basic, core-trigger, and compliance-specific data sets and their related data elements. We also reviewed DITPR IPT meeting notes that addressed data deficiencies, and performed queries of the DITPR database extract dated April 20, 2016. Our analysis focused primarily on core-trigger and compliance-specific data sets that supported E-Authentication, FISMA, PIA, PK Infrastructure, Privacy Act, Office of Management and Budget, and mission-criticality requirements because incomplete or missing data in these data sets, that are used for compliance reporting, carries a greater risk than incomplete or missing core-basic data. Through our reviews, we identified 2,992 IT systems in DITPR with incomplete core-trigger and compliance-specific data sets.

Incomplete Core-Trigger Data Set Information

Through our reviews of DITPR core-trigger data sets, we identified the following core-trigger data elements that the system owners did not complete.

- PK-Enabled core-trigger data element—the data element was not completed for 829 IT systems. The PK-Enabled core-trigger data element indicates whether the IT system is PK-Enabled.³⁰

³⁰ PK-Enabling involves replacing existing or creating new user authentication systems using certificates instead of other technologies, implementing PK technology to digitally sign transactions and documents, or using PK technology to encrypt information at rest or in transit.

- FISMA core-trigger data element—the data element was not completed for 43 IT systems. The FISMA core-trigger data element indicates whether the IT system requires security certification and accreditation for FISMA reporting.
- E-Authentication core-trigger data element—the E-Authentication core-trigger data element was not completed for 137 IT systems. This data element indicates whether the IT system is browser-based.
- Personal identifiable information core-trigger data element—the data element was not completed for 96 IT systems. The personal identifiable information core-trigger data element indicates whether the system contains information for PIA and Privacy Act reporting.

The responses that DoD Components provide in the core-trigger data sets determine whether system owners must complete related compliance-specific data sets in DITPR. By not completing these core-trigger data sets, DoD Components cannot properly address compliance-specific data sets for affected IT systems.

Incomplete Compliance-Specific Data Set Information

Through our reviews of DITPR compliance-specific data sets, we identified the following compliance-specific data elements that the system owners should have completed because they were mandatory or based on responses to core-trigger questions, but were not complete.

- Accreditation Not Required data element—this data element was not completed for 149 IT systems. The Accreditation Not Required data element indicates why the IT system did not require security certification and accreditation for FISMA reporting.
- Interfaces Identified data element—this data element was not completed for 653 IT systems. The Interfaces Identified data element indicates whether system interfaces between mission-critical and mission-essential IT systems and other systems have been identified.
- Hosting Environment³¹ data element—this data element was not completed for 1,130 IT systems. The Hosting Environment-specific data element indicates the hosting environment—area processing center, Defense Enterprise Computing Center or equivalent, core data center, information processing node, cloud, commercial, or other—in which the IT system operates.
- Data Center Name and Location data elements—the data elements were not completed for 1,138 IT systems. The Data Center Name and Location data elements indicate the location of the IT system's hosting environment.

³¹ A hosting environment is the physical environment that holds the data.

DoD CIO Did Not Properly Manage DITPR Data Quality

DoD Components did not report complete and accurate IT system data in DITPR because the DoD CIO did not hold Component CIOs accountable for ensuring the completeness and accuracy of data reported in DITPR, ensure DoD Components corrected errors identified during periodic data reviews, or require adequate DITPR training for DoD Component personnel.

No Accountability for Data Quality

The DoD CIO did not hold DoD Components accountable for ensuring the completeness and accuracy of data reported in DITPR. DITPR guidance required DoD Component CIOs to certify, in writing, that all system information reported in DITPR was accurate and complete. However, in a 2009 memorandum,³² the DoD CIO canceled those requirements, keeping only the more general certification that the Component CIOs complied with criteria. A DoD CIO official stated that the certification requirement was canceled because DoD Components were knowingly submitting inaccurate certification documents just to comply with DITPR guidance. Additionally, when asked for the most recent general certification from each Component, a DITPR analyst stated that in 2012, the DoD CIO had verbally canceled the general certification requirement. In addition, the DoD CIO official stated that the DoD CIO does not own DITPR data, and therefore lacks the authority to require DoD Components to ensure the data reported in DITPR were complete and accurate. However, IT system data and the procedures used by DoD Components to report those data in DITPR are part of the DoD information enterprise.³³ DoD guidance states that the DoD CIO:

The DoD CIO did not hold DoD Components accountable for ensuring the completeness and accuracy of data reported in DITPR.

- is responsible for all matters relating to the DoD information enterprise, which includes IT systems such as DITPR; and
- in performance of his or her duties assigned under Federal law,³⁴ will ensure compliance by DoD Component CIOs with DoD policy under the purview of the DoD CIO.³⁵

³² DoD CIO Memorandum, "DoD IT Portfolio Repository (DITPR) and DoD SIPRNET IT Registry Guidance," August 10, 2009.

³³ DoD Directive 8000.01, "Management of the DoD Information Enterprise (DoD IE)," March 17, 2016, defines the information enterprise as the DoD information resources, assets, and processes required to achieve an information advantage and to share information across DoD with mission partners.

³⁴ 10 U.S.C. § 2223 (2014) and 40 U.S.C. § 11315 (2014).

³⁵ DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014.

To properly manage DITPR data quality, the DoD CIO must hold DoD Components accountable for ensuring the completeness and accuracy of IT system data they report in DITPR. While the DoD CIO's data certification requirement did not work as intended, the DoD CIO needs to establish a process that holds DoD Component CIOs accountable for the completeness and accuracy of the data they report in DITPR.

DITPR Data Deficiencies Identified But Not Adequately Addressed

The DoD CIO identified DITPR data deficiencies but did not ensure that the DoD Components took action to correct them.

The DoD CIO identified DITPR data deficiencies but did not ensure that the DoD Components took action to correct them. DITPR guidance requires that the DoD CIO use DITPR-generated reports to identify deficiencies in the data reported by DoD Components. The DoD CIO notifies DoD Components of these deficiencies during monthly DITPR IPT meetings and performs trend analyses to track the deficiencies over time. However, the DoD CIO did not set deadlines for correcting deficiencies and did not follow up with DoD Components to ensure adequate corrective action was taken. For example, in May 2016, the DoD CIO reported that the U.S. Marine Corps had 13 systems with expired authority to operate.³⁶ Thirteen systems continued to be reported in June and July of 2016, and more systems were added in the following months. Control activities used by the DoD CIO to identify and track data deficiencies can only be effective if the deficiencies are addressed and corrected. Therefore, the DoD CIO needs to not only notify IT system owners of data deficiencies, but also set deadlines for correcting these deficiencies and regularly follow up with DoD Components to ensure resolution.

Inadequate DITPR Training

The DoD CIO did not require adequate DITPR training for DoD Component personnel. DITPR training consists of introductory training slides, user guides, and user guide updates. In addition, the DoD CIO communicates user guide updates to DoD Component CIOs and DITPR administrators via monthly DITPR IPT meetings. However, while DITPR training is readily available and useful for creating reports, the training is not required for users. For example, we identified that system representatives for two of five Office of the Secretary of Defense CIO IT systems reviewed had not taken DITPR training. We also identified that system owners reported inaccurate information in DITPR for all five of those IT systems.

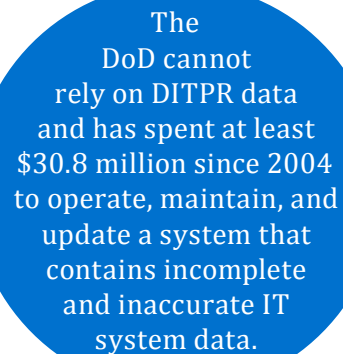
³⁶ An authority to operate is the official management decision issued by an authorizing official to authorize operation on an information system and to explicitly accept the residual risk to agency operations.

In addition, attendance at the DITPR IPT meetings was consistently low. Of the 78 DoD Component representatives invited to each of seven meetings held from April to October 2016, on average, only 27 (34.6 percent) attended.

Additionally, the introductory training presentation does not provide users with a clear understanding of DITPR's overall purpose, statutory requirements, or relationship to DoD Component feeder systems and does not communicate the importance of reporting complete and accurate IT system data in DITPR. For example, the DITPR training does not address the importance of accurately identifying interfaces or indicate there is a Congressional requirement for identifying interfaces in DITPR. If interfaces were accurately identified, the DoD CIO could effectively plan for or respond to disruptions in the operation of and between interfacing systems. However, owners for two IT systems that had interfacing systems reported no interfaces because these systems had large and greatly fluctuating numbers of system interfaces. Therefore, it is critical that the DoD CIO make DITPR training mandatory for all DITPR users and IT system owners. Additionally, the DoD CIO needs to add training content to increase awareness of DITPR's purpose, statutory requirements, and relationship to DoD feeder systems, and to emphasize the importance of reporting complete and accurate data in DITPR.

DITPR Information is Unreliable

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



The DoD cannot rely on DITPR data and has spent at least \$30.8 million since 2004 to operate, maintain, and update a system that contains incomplete and inaccurate IT system data.

Federal law and DoD guidance require the DoD CIO to maintain a consolidated inventory of mission-critical and mission-essential IT systems and identify interfaces between those systems and other IT systems for contingency planning purposes. Since 2004, the DoD CIO has used DITPR to meet these requirements. However, DITPR's inventory erroneously included IT systems, which misstates the number of IT systems in the DITPR inventory. Furthermore, inaccurate and incomplete interfacing system information limits DoD's ability to plan for IT system disruptions. Because disruptions in one IT system can result

in disruptions in interfacing systems, it is critical for contingency planning that interface data is accurate and complete. Unexpected disruption in the use of a mission-critical or mission-essential IT system could negatively impact warfighter operations or direct mission support for warfighter operations.

Additionally, the DoD cannot use DITPR as intended to make managerial, investment, and budget decisions. For example, in support of the Office of Management and Budget's Federal Data Center Consolidation Initiative, the DoD CIO performs cost analyses to identify and recommend DoD data center assets and locations for consolidation. This consolidation helps to maximize cost savings and minimize energy usage. The DoD CIO should be able to use hosting environment and data center name and location information in DITPR to support the cost analyses. However, 2,268 IT systems registered in DITPR as of April 20, 2016, did not have that information. Instead, the DoD CIO has had to use information from multiple sources—including data center site visits—to overcome the lack of hosting-related information in DITPR to perform the cost analyses.

Finally, DoD's statutory compliance reporting based on DITPR is inaccurate. This includes DoD's reporting on FISMA compliance to the Office of Management and Budget. The incomplete and inaccurate data we identified in DITPR adversely affect the DoD CIO's FISMA metrics used to measure the DoD's progress toward achieving outcomes that strengthen DoD and Federal cybersecurity. For example, IT systems erroneously included in DITPR misstate the DoD's total number of IT systems and the number of IT systems that are subject to FISMA reporting requirements.

Management Comments on the Finding and Our Response

Management Comments on DITPR as the Data Source for Obligated Funds

The Acting Principal Deputy, DoD CIO, commenting for the DoD CIO, recommended that we remove the draft report statement that DITPR is the data source used to report funds obligated for Defense Business Systems. The Acting Principal Deputy stated that the functionality related to funds obligated for Defense Business Systems was removed from DITPR in FY 2014 and is now accomplished in the DoD Information Technology Investment Portal.

Our Response

Our sources for the draft report statement were DITPR guidance, September 6, 2007, and the DITPR Data Dictionary.³⁷ Those references state that DITPR includes information used to meet the reporting requirements for Defense Business System obligated funds. However, on April 11, 2017, the DoD CIO distributed updated draft DITPR guidance for coordination that clarifies the relationship between DITPR and the DoD Information Technology Investment Portal. The 2017 draft guidance highlights that DITPR is not the primary source of obligated funds data needed to meet the reporting requirements of Defense Business Systems. Instead, the DoD Information Technology Investment Portal aligns IT system information in DITPR with funding information in the Select and Native Programming Data Input System for Information Technology to meet the requirements. Based on the updated draft DITPR guidance, we agreed to remove the statement from the report.

Management Comments on Ownership of DITPR Data

The Acting Principal Deputy, DoD CIO, commenting for the DoD CIO, also recommended that we remove the draft report statement from a DoD CIO official that the DoD CIO does not own DITPR data, and therefore lacks the authority to require DoD Components to ensure the data reported in DITPR were complete and accurate. The Acting Principal Deputy added that this is not the position of the DoD CIO and, therefore, the statement should be removed.

Our Response

We did not remove the statement because a senior DoD CIO *official* made the statement during an August 8, 2016, meeting. Specifically, we asked why the DoD CIO stopped requiring Component CIOs to submit memorandums certifying that their Components' IT system information reported in DITPR was accurate and complete. The DoD CIO *official* responded that because the DoD CIO does not own the IT system data, it lacks the authority to require Component CIOs to enter complete and accurate information. In the report, we correctly attribute the statement to a DoD CIO *official* and did not imply that it was the position of the DoD CIO.

³⁷ DITPR guidance states that the DITPR Data Dictionary is a working document that includes a matrix of data elements to be completed and is updated as changes to DITPR are approved.

Recommendations, Management Comments and Our Response

Recommendation 1

We recommend that the DoD Chief Information Officer:

- a. **Establish a process that holds DoD Component Chief Information Officers accountable for the completeness and accuracy of DoD Information Technology Portfolio Repository data.**

DoD Chief Information Officer Comments

The Acting Principal Deputy, DoD CIO, commenting for the DoD CIO, agreed, stating that DoD Components are responsible for the integrity, completeness, quality, and utility of information within DITPR. To improve the completeness and accuracy of DITPR data, the Acting Principal Deputy stated that, by the 4th Quarter FY 2017, the DoD CIO will initiate a semiannual data quality review process which will provide Component CIOs specific details on data deficiencies that need attention and will require Component CIOs to report on corrective actions. Additionally, the Acting Principal Deputy stated that the DoD CIO will monitor Component corrective actions as part of its data quality check presented during monthly DITPR Working Group meetings.³⁸ The monthly data quality check, which previously used summary level data, will now be detail focused.

- b. **Notify IT system owners of data deficiencies, give deadlines for corrections, and regularly follow up with DoD Components to ensure resolution;**

DoD Chief Information Officer Comments

The Acting Principal Deputy, DoD CIO, commenting for the DoD CIO, agreed, stating that, by the 4th Quarter FY 2017, the DoD CIO will initiate a more focused approach to notify DoD Components of data deficiencies and follow up to ensure correction. The Acting Principal Deputy added that, in conjunction with Recommendation 1.a, the approach would include notifying, providing suspense dates, and following up with DoD Components on a monthly basis to ensure resolution of data deficiencies.

Our Response

Comments from the Acting Principal Deputy addressed all specifics of the recommendations; therefore, the recommendations are resolved. The DoD CIO already notifies Components of data deficiencies as part of the data quality check presented during monthly DITPR IPT meetings. Setting deadlines for DoD

³⁸ DITPR Working Group is the same as the IPT.

Components to correct deficiencies and following up to ensure resolution in the monthly data checks, along with initiating a semiannual data quality review process, will enable the DoD CIO to hold DoD Component CIOs accountable for the completeness and accuracy of DITPR data and result in improved DITPR data quality. We will close the recommendations once we verify that the DoD CIO is establishing deadlines for correcting deficiencies at the monthly DITPR IPT meetings, following up to ensure resolution, and has initiated a semiannual data quality review process.

- c. **Require DITPR training for all DITPR users and IT system owners and add training content to increase awareness of DITPR's purpose, statutory requirements, relationship to DoD feeder systems, and the importance of reporting complete and accurate data in DITPR.**

DoD Chief Information Officer Comments

The Acting Principal Deputy, DoD CIO, commenting for the DoD CIO, partially agreed, stating that the DoD CIO will work with stakeholders to update the current training material to incorporate increased awareness of DITPR's statutory requirements, DITPR's relationship to DoD feeder systems, and the importance of reporting complete and accurate data. Additionally, the Acting Principal Deputy stated that by the 4th quarter FY 2017, the DoD CIO would update training material and request that all users complete DITPR training to obtain and maintain a DITPR account.

Our Response

Comments from the Acting Principal Deputy partially addressed the recommendation; therefore, the recommendation is unresolved. DITPR users and IT system owners may interpret a "request" to complete DITPR training to obtain and maintain a DITPR account as optional. Therefore, the DoD CIO should provide comments on the final report specifying how he will require that all DITPR users and system owners complete the necessary training.

Unsolicited Management Comments on the Recommendations and Our Response

Department of the Navy Comments

Although not required to comment, we received an e-mail from a Department of the Navy, CIO representative stating that the Department of the Navy CIO concurred with the draft report recommendations.

Defense Information Systems Agency Comments

Although not required to comment, the Defense Information Systems Agency CIO concurred with the draft report recommendations and stated that the DoD CIO should establish a process that supports improved accuracy and completeness of data in DITPR. He further stated that the Defense Information Systems Agency had already implemented a process of notification, deadlines for corrections, and follow-up for data elements identified through the DITPR IPT and will continue to conduct training for DITPR users.

Our Response

We appreciate the unsolicited comments received from the Department of the Navy and the Defense Information Systems Agency. We commend the Defense Information Systems Agency for taking actions to improve their data entry processes to ensure the accuracy and completeness of DITPR data.

Appendix

Scope and Methodology

We conducted this performance audit from March 2016 through February 2017 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.

We reviewed relevant Federal and DoD guidance related to DITPR. We also reviewed current and draft DITPR guidance, military feeder system guidance, and DITPR IPT meeting minutes. We met with DoD and other Component CIOs to discuss their roles and responsibilities and internal controls related to DITPR reporting and maintenance. We obtained access rights to DITPR and on April 20, 2016, extracted a universe of 6,169 active IT systems listed in DITPR. We also attended monthly IPT meetings held from April 2016 to December 2016.

To determine whether DITPR data entries were accurate, we selected a nonstatistical sample of 35 IT systems from the April 20, 2016 DITPR data extract that were listed as MAC I systems and that were geographically concentrated to minimize travel costs.³⁹ We reviewed DITPR system information for each of the selected IT systems. We also met with system program managers, information security system managers, and other system personnel for 31 of the 35 sample IT systems (we did not review four of the IT systems because there was sufficient evidence to support our audit conclusions after reviewing 31). In those meetings, we verified the DITPR information and obtained supporting documentation related to FISMA, PIA, Privacy Act, E-Authentication, and interfacing requirements. We conducted site visits to Wright-Patterson Air Force Base, Ohio; Scott Air Force Base, Illinois; and St. Louis, Missouri.

To determine whether DoD Components reported complete IT system data in DITPR, we performed queries of the April 20, 2016 data extract. The queries were designed to identify incomplete data fields. Specifically, we focused on core-trigger and compliance-specific data sets that contained information that supported FISMA, PIA, Privacy Act, PK Infrastructure, E-Authentication, and Office of Management and Budget requirements.

³⁹ Our sample did not include top-secret systems. According to DoD CIO officials, the unclassified DITPR includes systems that process classified information provided that only unclassified system information is used when registering a system and nothing classified is disclosed.

Use of Computer-Processed Data

We used computer-processed data to perform this audit. Specifically, we extracted data reports from DITPR and compared them to supporting documents received, information received during interviews with system representatives, and excerpts from the military IT feeder systems to determine whether DITPR data were accurate and complete. Since DITPR is a data repository, we determined that errors in DITPR were due to data entry input errors as discussed in our finding, not DITPR processing deficiencies. Therefore, we determined that the data in DITPR were sufficiently reliable for our sampling selection because our audit would determine the accuracy and completeness of the data.

Use of Technical Assistance

We initially coordinated with the DoD Office of Inspector General (DoD OIG), Quantitative Methods Division, to develop a statistical sample of 157 IT systems in DITPR to test for completeness and accuracy. However, our preliminary results indicated that a smaller sample would sufficiently answer our audit objective. Therefore, the audit team developed a nonstatistical sample of IT systems in DITPR to test for completeness and accuracy.

Prior Coverage

During the last 5 years, the DoD OIG and the Army Audit Agency issued two reports discussing DITPR or DITPR-related topics. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/pubs/index.cfm>. Unrestricted Army Audit Agency reports can be accessed from .mil domains at <https://www.aaa.army.mil/>.

DoD OIG

Report No. DoDIG-2016-068, “DoD’s Efforts to Consolidate Data Centers Need Improvement,” March 29, 2016

The audit objective was to determine whether selected DoD Components were effectively consolidating their data centers in accordance with the Federal Data Center Consolidation Initiative. The DoD OIG determined that DoD Components did not accurately report data center information to the DoD CIO. The DoD OIG recommended that the DoD CIO develop and issue comprehensive guidance for accurately reporting data center information in the Data Center Inventory Management system. The DoD OIG also recommended that the DoD CIO develop a process for validating the accuracy and completeness of information in the Data Center Inventory Management system. The DoD OIG further recommended

that the CIO, Department of the Army; Department of the Navy CIO; CIO, Office of the Secretary of the Air Force; and the CIO, Defense Information Systems Agency, revise their current processes for validating data center information to ensure the accuracy and completeness of information reported to the DoD CIO.

Army Audit Agency

Report No. A-2016-0062-IET, "Data Reliability in the Army Portfolio Management Solution," March 22, 2016

The audit objective was to verify that the Army Portfolio Management Solution (APMS)⁴⁰ had reliable IT system information to enable Army leaders to satisfy reporting requirements and to make informed management decisions. The Army Audit Agency found that all 17 APMS data fields it reviewed had inaccuracies or incomplete or illogical responses. The Army Audit Agency recommended that the Army CIO/G-6 identify other data sources that can feasibly integrate with APMS, define APMS data elements, update and communicate APMS guidance, improve APMS training, and implement data field controls within APMS.

⁴⁰ APMS is the Army's feeder system for DITPR reporting.

Management Comments

DoD Chief Information Office



CHIEF INFORMATION OFFICER

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

APR 10 2017

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Draft Report "DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository" (Project No. D2016-D000R-0129.000)

DoD CIO reviewed the DoD IG Draft Report, "DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository" (Project No. D2016-D000R-0129.000), and our response is attached.

My point of contact is Mr. William Guthrie, [REDACTED]

A blue ink signature of Thomas P. Michelli.

Thomas P. Michelli
Acting Principal Deputy

Attachment:
As stated

DoD Chief Information Office (cont'd)

Department of Defense (DoD) Comments on DoD IG Draft Report, 'DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository' (Project No. D2016-D000RA-0129.000)

Recommended Corrections to DoD IG Draft Report:

Reference page 2, 3rd bullet. Delete bullet. Report of funds obligated for Defense Business Systems is accomplished in the DoD Information Technology Investment Portal (DITIP). This functionality was removed from DITPR in FY14.

Reference page 11, 2nd paragraph. Delete statement "In addition, the DoD CIO official stated that the DoD CIO does not own DITPR data, and therefore lacks the authority to require DoD Components to ensure the data reported in DITPR are complete and accurate." This is not the DoD CIO position and should be removed from the report.

Response to DoD IG Draft Report Recommendations:

Recommendation (a): Establish a process to hold DoD CIOs accountable for the completeness and accuracy of DITPR data.

DoD Response: Concur. DoD CIO has stated through Memorandum, Guidance, and draft DoD Manual that DoD Components are responsible for the integrity, completeness, quality, and utility of information within DITPR. To improve the completeness and accuracy of DITPR data, DoD CIO will initiate a semi-annual data quality review process which will provide specific details on data deficiencies to Component CIOs for them to fix and report on corrective actions. DoD CIO will monitor Component corrective actions as part of its monthly data quality check (previously done with summary level data; now will be detail focused) as part of the monthly DITPR Working Group meeting. Target timeframe for the first semi-annual data quality review is 4th Quarter, FY17.

Recommendation 1(b): Notify IT system owners of data deficiencies, give deadlines for correction, and regularly follow up with DoD Components to ensure resolution.

DoD Response: Concur. DoD CIO will initiate a more focused approach to notifying and following up to ensure correction of Components data. In conjunction with recommendation 1(a), the process will include notification, suspense date, and following up with DoD Components to ensure resolution of data deficiencies. Target timeframe is 4th Quarter FY17.

Recommendation 1(c): Require DITPR training for all DITPR users and IT system owners and add training content to increase awareness of DITPR's purpose, statutory requirements, relationships to DoD feeder systems, and the importance of reporting complete and accurate data in DITPR.

DoD Response: Partially concur. Training material already exists on-line in the form of video, briefings, and user manual on various aspects of DITPR functionality. DoD CIO will

DoD Chief Information Office (cont'd)

work with PMW240 to update the current training material to incorporate increase awareness of DITPR's statutory requirements, relationship to DoD feeder systems, and importance of reporting complete and accurate data for the DoD Components who enter data directly into DITPR. We will also work with the Military Departments responsible for their Component feeder systems. Once the training material is updated, DoD CIO will request all user's complete training as a condition to obtaining/maintaining a DITPR account. Target timeframe is beginning 4th Quarter FY17.

Defense Information Systems Agency



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

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: DISA's comments to Draft Report on DoD Components Did Not Report Complete and Accurate Data in the DoD Information Technology Portfolio Repository, February 23, 2017 (Project No. 2016-D000RA 0129.000)

The Defense Information Systems Agency has reviewed the final report referenced above and provides comments, as attached. These comments are meant to provide clarity to the recommendations. We thank the DoD IG audit team for the recommendations made in the final report and hope the additional information provided will complete this task.

We look forward to continuing to work with you and your staff in the future. Any questions your staff may have concerning matters for the recommendation should be directed to Mr. Hector Lorenzo [REDACTED] or Mr. Patrick Webb, [REDACTED]. Please do not hesitate to contact them should you need to further discuss this matter.

BENNETT DAVID B
ENJAMIN 10713044
49

DAVID B. BENNETT
Chief Information Officer

1 Attachment
DISA Comments to DoD IG

Defense Information Systems Agency (cont'd)

**DOD IG Draft REPORT NO. DODIG-2016-D000RA, DATED FEBUARY
23, 2017 (Project No. 0129.000)**

**“DoD Components Did Not Report Complete and Accurate Data in the DoD Information
Technology Portfolio Repository”**

DEFENSE INFORMATION SYSTEMS AGENCY COMMENTS TO DOD IG RECOMMENDATIONS

RECOMMENDATION: We recommend that the DoD Chief Information Officer: a. Establish a process that holds DoD Component Chief Information Officers accountable for the completeness and accuracy of DITPR data; b. Notify IT system owners of data deficiencies, give deadlines for corrections, and regularly follow up with DoD Components to ensure resolution; and c. Require DITPR training for all DITPR users and IT system owners and add training content to increase awareness of DITPR’s purpose, statutory requirements, relationship to DoD feeder systems, and the importance of reporting complete and accurate data in DITPR.

DISA RESPONSE: Concur with comments

DISA concurs that the DOD CIO should establish a process that supports improved accuracy and completeness of data in DITPR. Developing a DOD CIO process that holds system owners directly accountable for information in DITPR would improve DITPR data. DOD CIO should model a process similar to the Defense Business System process of certifying funds. The certification of funds process requires accurate DITPR reporting to successfully proceed to the next phase of system lifecycle.

DISA has already implemented a process of notification, deadlines for corrections, and follow-up for data elements identified through the DITPR IPT and will continue to conduct training for DITPR users as recommended.

The Action Officer for DITPR information is Mr. Patrick Webb, [REDACTED]
[REDACTED]

Acronyms and Abbreviations

APMS	Army Portfolio Management Solution
CIO	Chief Information Officer
DITPR	DoD Information Technology Portfolio Repository
FISMA	Federal Information Security Modernization Act
IPT	Integrated Process Team
IT	Information Technology
MAC	Mission Assurance Category
NSS	National Security System
PIA	Privacy Impact Assessment
PK	Public Key
U.S.C.	United States Code



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/programs/whistleblower.

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

Congressional Liaison

congressional@dodig.mil; 703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

For Report Notifications

www.dodig.mil/pubs/email_update.cfm

Twitter

www.twitter.com/DoD_IG

DoD Hotline

www.dodig.mil/hotline



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

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

