Report No. DODIG-2019-037

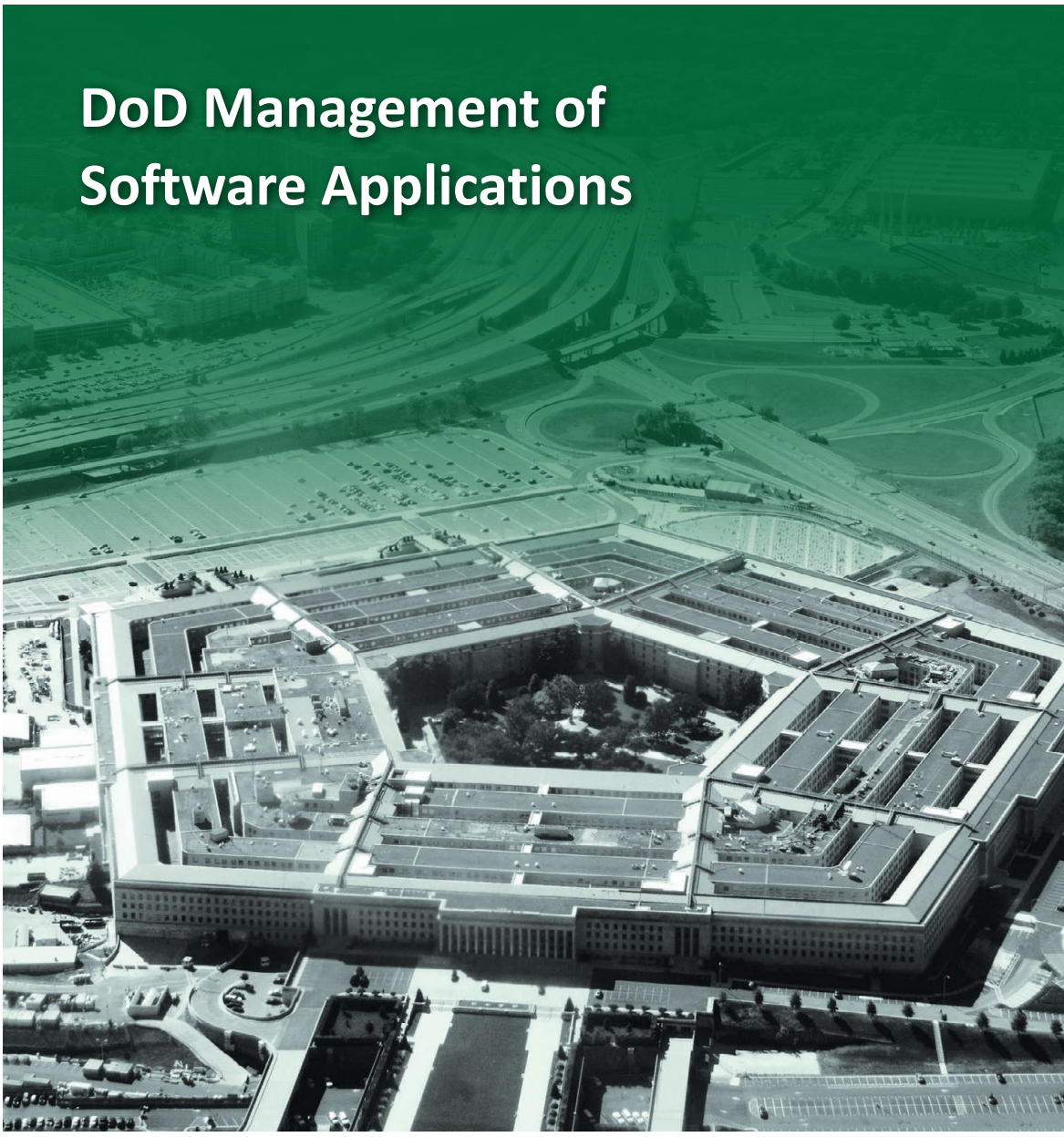
~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

DECEMBER 13, 2018

DoD Management of Software Applications



INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

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

~~FOR OFFICIAL USE ONLY~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Results in Brief

DoD Management of Software Applications

December 13, 2018

Objective

We determined whether DoD Components rationalized their software applications by identifying and eliminating any duplicative or obsolete applications. This audit focused on the Marine Corps, the Navy, and the Air Force. We did not include the Army in our audit scope because the Army Audit Agency reviewed software application inventories and software application rationalization at its data centers.[1]

Background

A software application is a program that performs a specific function for a user, such as office automation, e-mail, or web services. Software application rationalization is the process of optimizing an enterprise's information technology portfolio by:

- identifying all software applications owned and in use on the enterprise networks;
- determining whether existing software applications are needed, duplicative, or obsolete based on mission objectives and costs; and
- determining whether a software application already exists within the enterprise before purchasing applications.

Finding

The Marine Corps, the Navy, and the Air Force commands and divisions we reviewed did not consistently rationalize their software applications. Although the Marine Corps divisions and the Navy commands had a process in place to prevent duplication when purchasing software applications, the Air Force did not. In addition, the U.S. Fleet Forces Command was the only command we reviewed that had a process in place for eliminating duplicative or obsolete software applications it owned. Furthermore, none of the commands or divisions we reviewed maintained accurate software inventories to facilitate that process.

[1] Report No. A-2017-0099-IET, "Army Data Center Closure Reports," September 28, 2017.

Finding (cont'd)

This occurred because the DoD Chief Information Officer (CIO) did not implement an enterprise-wide solution for software application rationalization in response to Federal Information Technology Acquisition Reform Act requirements and, instead, limited rationalization to data center consolidation efforts.

As a result, the DoD and its Components are exposing the DoD Information Network to unnecessary cybersecurity risks because they lack visibility over software application inventories and, therefore, are unable to identify the extent of existing vulnerabilities associated with their owned software applications. In addition, the DoD is not realizing the cost savings associated with the elimination of duplicate and obsolete software applications that it has already procured and is paying to maintain.

Recommendations

We recommend that the DoD CIO, in coordination with the DoD Chief Management Officer:

- develop an enterprise-wide process for conducting the software application rationalization process throughout the DoD;
- establish guidance requiring the DoD Components to conduct software application rationalization and require DoD Component CIOs to develop implementing guidance that outlines responsibilities and processes for software application rationalization within their Components. The policy should also require DoD Components to regularly, at least annually, validate the accuracy of their owned and in use software applications inventory; and
- conduct periodic reviews to ensure that DoD Components are regularly validating the accuracy of their inventory of owned and in use software applications and that DoD Components are eliminating duplicate and obsolete software applications.

Management Comments and Our Response

The DoD CIO did not provide a response to recommendations in a draft of this report; therefore, the recommendations are unresolved. We request that the DoD CIO provide comments on the final report.

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

Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Chief Information Officer, Department of Defense	1.a, 1.b, 1.c	None	None

Please provide Management Comments by January 11, 2019.

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

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

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

December 13, 2018

MEMORANDUM FOR DOD CHIEF MANAGEMENT OFFICER
DOD CHIEF INFORMATION OFFICER
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: DoD Management of Software Applications (Report No. DODIG-2019-037)

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

DoD Instruction 7650.03 requires that recommendations be resolved promptly. The DoD Chief Information Officer did not provide a response to recommendations in a draft of this report. We request that the DoD Chief Information Officer provide comments to the final report by January 11, 2019.

Please send a PDF file containing your comments on the recommendation to CSO@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. 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 (703) 699-7331 (DSN 499-7331).

Carol N. Gorman
Assistant Inspector General
Cyberspace Operations

Contents

Introduction

Objective

We determined whether the DoD Components rationalized their software applications by identifying and eliminating any duplicative or obsolete applications.

For this audit, we focused on the Marine Corps, the Navy, and the Air Force. We did not include the Army because the Army Audit Agency issued report A-2017-0099-IET, "Army Data Center Closure Reports," September 28, 2017. In that report, the Army Audit Agency reviewed software application inventories and software application rationalization at Army data centers. The Army Audit Agency made a recommendation to the Army CIO related to the reporting of cost savings associated with software application rationalization for data centers. See Appendix A for a discussion on the scope and methodology and prior audit coverage. See the Glossary for definitions of technical terms.

Background

A software application is a program that performs a specific function for a user, such as office automation, e-mail, or web services. Software application rationalization is the process of improving an enterprise's information technology portfolio by:

- identifying all software applications owned and in use on the enterprise networks. The types of software applications used within the DoD include commercial off-the-shelf (COTS), Government off-the-shelf, and open source software applications;
- determining whether existing software applications are needed, duplicative, or obsolete based on mission objectives and costs, and taking appropriate actions to keep or eliminate software applications based upon objectives, resource availability, mission impact, business impact, and dependencies; and
- determining whether a software application already exists within the enterprise before purchasing applications.[2]

[2] DoD Directive 8115.01, "Information Technology Portfolio Management," October 10, 2005, defines an information technology portfolio as a group of information technology investments, aligned by capability, to accomplish a specific functional goal, objective, or mission outcome.

COTS software is ready-made by commercial vendors and available for sale, lease, or license to the public, as well as to the U.S. Government.

Government off-the-shelf software is Government-produced applications and COTS software that has been modified to provide the Government a specific capability and is retained and maintained inside the U.S. Government.

Open source software is software that is available in source code form, which allows code level modification and customization by vendors or programs for specific uses.

The benefits of software application rationalization include identifying opportunities for cost savings, minimizing excessive or unneeded software application purchases, and eliminating unnecessary investments.

Federal and DoD Guidance

Federal and DoD guidance include the following requirements to optimize information technology portfolios, programs, and resources, including software applications.

- **Executive Order No. 13589, 76 Fed. Reg. 70,861 (2011)** requires Federal agencies to assess their inventories and usage of their current devices and establish controls to ensure that they are not paying for unused or underutilized installed software.
- **Federal Information Technology Acquisition Reform Act (FITARA) of FY 2015** requires CIOs to review their agency information technology portfolios and develop a multiyear strategy to identify and reduce duplication and waste within the portfolios, including component-level investments and software.[3] In June 2015, the Office of Management and Budget (OMB) issued implementation guidance for FITARA, with a requirement for PortfolioStat.[4] PortfolioStat is a quarterly review of information technology portfolio management for Federal agencies that is conducted by the agency CIOs and senior agency officials.[5] Based on lessons learned from PortfolioStat results, the OMB recommended that Federal agencies rationalize their software application inventory as an enterprise-wide approach.[6]
- **DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," March 12, 2014 (Incorporating Change 2, July 28, 2017),** requires DoD Components to implement security controls from the National Institute of Standards and Technology Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013 on all of their information systems. Special Publication 800-53 requires the DoD to develop, review, and update an inventory of information system components, including software applications.

[3] Public Law 113-291, "The National Defense Authorization Act for Fiscal Year 2015," subtitle D, "Federal Information Technology Reform Act," section 833, "Portfolio Review," December 19, 2014. National security systems are exempt from Public Law 113-291, section 833.

[4] OMB Memorandum M-15-14, "Management and Oversight of Federal Information Technology," June 10, 2015.

[5] PortfolioStat requirements apply to agencies listed in 31 U.S.C. §901 (b)(1) and (b)(2).

[6] The House Committee on Oversight and Government Reform worked with the Government Accountability Office to develop the FITARA scorecard to assess agencies' FITARA implementation efforts. The DoD received an F rating in PortfolioStat on its most recent (May 2018) FITARA scorecard.

Management of Software Applications

DoD Directive 8115.01 requires DoD Components to manage all of their information technology investments as portfolios. The DoD's enterprise portfolio is divided into four mission area portfolios: 1) warfighting, 2) business, 3) the DoD portion of intelligence, and 4) enterprise information environment. The DoD Chief Management Officer (CMO), the DoD CIO, and the DoD Components have specific responsibilities for information technology portfolio management.

DoD Chief Management Officer

The DoD CMO is the principal advisor to the Secretary of Defense on establishing policies for, and directing, all business operations of the Department. The CMO is also responsible for overseeing implementation of reform initiatives.[7] The DoD Reform Initiative efforts include renegotiating contracts, realigning and streamlining business processes, and taking inventory to enhance visibility of data surrounding information technology usage and spending.

DoD Chief Information Officer

The DoD CIO is the senior advisor to the Secretary of Defense for information technology matters and is responsible for all matters related to the DoD information enterprise, including network and cybersecurity policy and standards. The DoD CIO is also responsible for maintaining a consolidated inventory of DoD mission-critical and essential information systems, identifying opportunities for improving information technology efficiencies, and eliminating duplicate systems and software applications.

Department of the Navy

The Department of the Navy (DON) CIO is responsible for all matters related to information technology for the Marine Corps and the Navy. The Director, Command, Control, Communications, and Computers serves as the Deputy DON CIO and as the Marine Corps CIO, and is responsible for the governance, portfolio management, and investment decisions of the Marine Corps' enterprise. The Deputy Chief of Naval Operations for Information Warfare serves as the Deputy DON CIO and is responsible for aligning and integrating information technology portfolio management efforts through functional area managers (FAM) for the Navy's enterprise.

[7] In 2017, the Secretary of Defense directed DoD to conduct a thorough business review to identify viable reform initiatives to achieve the business reforms necessary to restore readiness in nine lines of business including cyber defense and information technology management.

The Marine Corps and Navy FAMs oversee the management, reduction, and consolidation of information systems and software applications and direct their migration, consolidation, or retirement consistent with applicable laws and regulations within their functional areas.

Department of the Air Force

The Chief, Information Dominance and CIO (SAF/CIO A6), is the principal advisor to the Secretary of the Air Force (SAF) for information technology matters. The SAF/CIO A6 has overall responsibility for network policies, communications, portfolio management, information resources management, information assurance, and related matters. Air Force portfolio managers are responsible for ensuring that information technology investments align to business strategies and support the elimination of duplicative investments.

Marine Corps, Navy, and Air Force Commands and Divisions Reviewed

For the audit, we visited the following Marine Corps, Navy, and Air Force commands and divisions.

- Marine Corps Command, Control, Communications, and Computers Network Plans and Policy Division; Washington, D.C.
- Marine Corps Logistics Plans, Policy, and Strategic Mobility Division; Washington, D.C.
- Naval Sea Systems Command (NAVSEA); Washington, D.C.
- Naval Facilities Engineering Command (NAVFAC); Washington, D.C.
- U.S. Fleet Forces Command (USFF); Norfolk, Virginia
- Air Force Materiel Command; Wright-Patterson Air Force Base, Ohio
- Headquarters Air Force CIO Support Division; Washington, D.C.

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.[8] We identified internal control weaknesses related to the DoD's processes for software application rationalization. Specifically, the DoD Components did not consistently rationalize their software applications to identify and eliminate duplicative or obsolete applications. We will provide a copy of the report to the senior officials responsible for internal controls within the Marine Corps, the Navy, the Air Force, and the Office of the DoD CIO.

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

Finding

DoD Components Did Not Consistently Rationalize Their Software Applications

The Marine Corps, the Navy, and the Air Force commands and divisions we reviewed did not consistently rationalize their software applications. Although the Marine Corps divisions and Navy commands had a process in place to prevent duplication when purchasing software applications, the Air Force did not. In addition, USFF was the only command we reviewed that had a process in place for eliminating duplicative or obsolete applications it owned. Furthermore, none of the commands or divisions we reviewed maintained accurate software inventories to facilitate that process.

This occurred because the DoD CIO did not implement an enterprise-wide solution for software application rationalization in response to FITARA requirements and, instead, limited rationalization to data center consolidation efforts.

As a result, the DoD and its Components are exposing the DoD Information Network to unnecessary cybersecurity risks because they lack visibility over software application inventories and, therefore, are unable to identify the extent of existing vulnerabilities associated with their owned software applications. In addition, the DoD is not realizing cost savings associated with the elimination of duplicate and obsolete software applications that it has already procured and is paying to maintain.

DoD Components Did Not Have Standardized Processes to Rationalize Their Software Applications

The Marine Corps, the Navy, and the Air Force commands and divisions we reviewed did not have standardized processes to rationalize their software applications. The Marine Corps divisions and Navy commands had a process in place to prevent duplication when acquiring software applications, but the Air Force did not. In addition, USFF was the only command we reviewed that had a process in place for eliminating duplicative or obsolete applications it owned. Furthermore, none of the commands or divisions maintained accurate software inventories to facilitate that process.

The Marine Corps Divisions and Navy Commands Had a Process to Prevent the Acquisition of Duplicate Software Applications

The Marine Corps divisions and Navy commands had a process in place to prevent the purchase of duplicate software applications but the Air Force did not. The Marine Corps divisions' and Navy commands' processes for preventing the purchase of duplicate software applications are explained in the following table.

Table. Marine Corps and Navy Processes to Prevent the Purchase of Duplicate Software Applications

Command/Division	System/Database	Process
Marine Corps Command, Control, Communications, and Computers Network Plans and Policy Division and Marine Corps Logistics Plans, Policy, and Strategic Mobility Division	DON Application and Database Management System (DADMS) Questionnaire*	Before FAMs approve a software application request, the requestors complete a DADMS questionnaire and submit it to the FAMs for review. The questionnaire includes the anticipated number of users, existing software applications it may replace, and cost. FAMs review the responses to determine whether to approve the software application request.
NAVSEA	Caucus Site Dashboard and DADMS	The NAVSEA CIO and FAM team review and approve requests to use software applications on the NAVSEA network. Before a request is approved, the NAVSEA CIO and FAM team review DADMS to determine whether the requested software application is a duplicate of software already in their portfolio. The review is completed in the Caucus Site, a dashboard that lists whether the NAVSEA CIO and FAM review team approved a software application for use and the rationale for the decision.
NAVFAC	Software application catalog maintained in NAVFAC Information Technology Enterprise Portfolio	Before requesters submit a software application request for approval, they review the NAVFAC software application catalog to determine if an existing application meets their current needs. Before approving a request, the NAVFAC portfolio manager also reviews the catalog and asks the requestors a series of questions to ensure that the requested software application is not already on the network. The catalog includes all NAVFAC managed software included in DADMS.
USFF	DADMS Questionnaire	Before FAMs approve a software application request, the requestor completes a DADMS questionnaire and submits it to the USFF portfolio manager. The USFF portfolio manager reviews the request for completeness and forwards it to the responsible FAM who approves or disapproves the new application request in DADMS. The questionnaire includes the planned software application network location, its purpose, and anticipated number of users.

* DADMS is the DON authoritative data source for information technology applications and database portfolio management.

Source: The DoD OIG.

DoD Components Did Not Have a Process to Eliminate Duplicate or Obsolete Software Applications

Only one of the commands and divisions we reviewed had a process in place for eliminating duplicative or obsolete software applications it owned. Specifically, the USFF had a process to identify duplicate software applications after they were purchased; however, the process did not consider whether the software applications were installed or used on the network. Secretary of Navy Instruction 5000.36A requires FAMs to eliminate duplicate and obsolete software applications; Marine Corps Order 5230.21 requires FAMs to evaluate applications within their portfolio to identify and validate capability gaps and eliminate unnecessary or duplicate capabilities; and Air Force Instruction 17-110 requires the SAF/CIO A6 Cyberspace Capabilities and Compliance Directorate to ensure the elimination of duplication within its information technology portfolio.[9]

A comprehensive inventory is key to determining whether duplicate or obsolete software exists. However, none of the commands or divisions maintained a comprehensive inventory of the software applications installed on their networks. DoD Instruction 8530.01 requires DoD Components to capture, correlate, analyze, and provide continuous visibility into DoD assets, including software applications.[10] Secretary of the Navy Instruction 5230.14 requires Marine Corps and Navy FAMs to maintain an inventory of investments, including software applications, on their official portfolio management system of record.[11] The FAMs consider DADMS as the system of record; however, DADMS only contains a list of approved and disapproved software applications, not the software applications actually installed on the network. Therefore, DADMS cannot be used to identify duplicate, underutilized, or obsolete software applications in use.

Air Force Instruction 17-110 states that the Information Technology Investment Portfolio Suite is the Air Force's enterprise authoritative source to document information technology portfolio compliance and budget. The Information Technology Investment Portfolio Suite is intended to be a central repository for all Air Force information technology data. We reviewed the Information Technology Investment Portfolio Suite and determined that it did not include a list of software applications in use on the network; therefore, we could not use it to identify duplicate or obsolete software in use on the network.

---

[9] Secretary of the Navy Instruction 5000.36A, "Department of the Navy Information Technology Applications and Data Management," December 19, 2005. Marine Corps Order 5230.21, "Information Technology Portfolio Management," October 3, 2012. Air Force Instruction 17-110, "Information Technology Portfolio Management and Capital Planning and Investment Control," May 23, 2018.

[10] DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016.

[11] Secretary of the Navy Instruction 5230.14, "Information Technology Portfolio Management Implementation," November 9, 2009.

On February 1, 2012, the Air Force Audit Agency recommended that the Air Force update its policies and assess its methods for information technology duplication reviews.[12] In September 2014, in response to the Air Force Audit Agency's recommendation, the Air Force Chief Technology Officer requested a pilot study to evaluate an automated tool for software application discovery and to produce a master list of software applications across the Air Force enterprise. The pilot study used an application discovery tool to identify and categorize software applications at seven Air Force installations. The application discovery tool had a library of functions that recognizes parts of known COTS products and if requested, could identify other types of software. The pilot study was completed in March 2017. The discovery tool was successful for COTS applications, but the tool did not recognize Government off-the-shelf or lesser-known software products; therefore, it could not be used to develop a comprehensive inventory of software applications.[13]

DoD CIO Did Not Implement an Enterprise Solution for Software Application Rationalization

The Marine Corps, the Navy, and the Air Force commands and divisions we reviewed did not consistently rationalize software applications because the DoD CIO did not implement an enterprise-wide solution for software application rationalization in response to FITARA requirements and, instead, limited rationalization to data center consolidation efforts. FITARA requires that agencies identify or develop ways to increase efficiencies of information technology investments, identify potential duplication, identify waste or cost savings, and develop action plans to improve the information technology portfolio. Although the DoD Components had elements of software rationalization in place, the DoD does not have guidance requiring a standardized, enterprise-wide approach to software application rationalization.

In August 2010, the Secretary of Defense announced a DoD-wide Efficiencies Initiative to move defense institutions toward a more efficient, effective, and cost-conscious way of doing business.[14] As part of the Initiative, the Secretary of Defense directed the consolidation of information technology infrastructure to achieve savings in acquisition, sustainment, and manpower costs and to improve the DoD's ability to execute its missions while defending its networks against growing cyber threats. To achieve that consolidation and improve cybersecurity, the DoD established the Joint Information Environment. One of

[12] Report No. F2012-0004-FB2000, "Information Technology Duplication Identification Process," February 1, 2012.

[13] Institute for Defense Analyses, "Pilot Study on Tools for Information Technology Asset Inventory Collection and Application Discovery, Volume 1," March 2017.

[14] Gates, Robert M., (2010). Statement on Department Efficiencies Initiative, <http://archive.defense.gov/Speeches/Speech.aspx?SpeechID=1496>, accessed on September 25, 2018.

the Joint Information Environment initiatives was to conduct software application rationalization across the DoD enterprise to identify and eliminate systems inventory by identifying software no longer used or needed. However, in 2017, the DoD revised the Joint Information Environment objective to state that rationalization would be limited to the data centers, which does not include the entire DoD enterprise. DoD CIO officials stated that the Joint Information Environment objective was revised because the Joint Information Environment scope was intended to address DoD's information technology infrastructure. Therefore, software application rationalization was only considered as it related to infrastructure, in this case, data centers.

An enterprise-wide approach to software application rationalization is needed to reduce duplication and identify cost savings across the DoD. The approach should include all software applications to ensure that the DoD obtains the maximum benefits from its rationalization efforts. Therefore, the DoD CIO, in coordination with the DoD CMO, should develop an enterprise-wide process for conducting software application rationalization. Once the process is developed, the DoD CIO, in coordination with the DoD CMO, should establish guidance requiring the DoD Components to conduct software application rationalization, and the DoD Component CIOs should develop implementing guidance that outlines responsibilities and processes for software application rationalization within their Components. In addition, the policy should also require DoD Components to regularly, at least annually, validate the accuracy of their owned and in use software applications inventory.

Software application rationalization should be a continuous process that requires regular re-evaluation to determine the effectiveness of the portfolio and its alignment with organizational objectives. Therefore, the DoD CIO, in coordination with the DoD CMO, should conduct periodic reviews to ensure that the DoD Components are regularly validating the accuracy of their inventory of owned and in use software applications and that DoD Components are eliminating duplicate and obsolete applications.

Duplicative and Obsolete Software Applications Lead to Unnecessary Cybersecurity Risks and Support Costs

The DoD and its Components are exposing the DoD Information Network to unnecessary cybersecurity risks by having duplicative or obsolete software applications on their networks.

In a July 10, 2018 memorandum to DoD officials, the DoD CIO stated that the DoD has yet to report over 30 percent of its software inventory.[15] Because the reporting of software inventory for the congressional software inventory reporting cycle is not complete, the DoD and its Components lack visibility over their assets and, therefore, are unable to determine the extent of existing vulnerabilities that could impact operations if information processed, stored, or transmitted by software applications is compromised. Protecting software applications against cybersecurity risks consists of implementing cyber hygiene practices, such as patching authorized software and deploying anti-virus software.

~~(FOUO)~~ [redacted]. Actively conducting software application rationalization across the DoD enterprise will ensure that duplicate, underutilized, and obsolete software is regularly identified with the associated cost savings.

It is important for the DoD to consistently conduct software application rationalization across its enterprise to reduce the risk of buying and building systems that are duplicative and unnecessarily costly to maintain and integrate. Furthermore, the DoD may be paying support costs such as maintenance costs for security patches, software fixes, and general updates for unnecessary software applications and not realizing the cost savings associated with eliminating them.

Management Actions Taken

The July 10, 2018 DoD CIO memorandum, emphasized the need to improve compliance with congressional software inventory reporting requirements and required the DoD to show significant improvement in reporting software inventory by December 2018. Specifically, the DoD CIO instructed the DoD Components to deploy and use existing software inventory modules to increase the DoD's known software inventory. The DoD CIO stated that the DoD must be able to identify, through automated means, the quantity of installed applications

[15] DoD CIO Memorandum, "National Defense Authorization Act, Fiscal Year 2017, Section 1653 Compliance, Information Security Continuous Monitoring, Implementing Comply-to-Connect Policy, and Limitations on Software Licensing," July 10, 2018.

and to provide the software inventory to a server or reporting service. Because the DoD CIO took action to improve DoD software inventory reporting during our audit, we are not making recommendations to the DoD Components to improve the accuracy of their software application inventories.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the DoD Chief Information Officer, in coordination with the DoD Chief Management Officer:

a. Develop an enterprise-wide process for conducting the software application rationalization process throughout the DoD.

b. Establish guidance requiring DoD Components to conduct software application rationalization and require DoD Component Chief Information Officers to develop implementing guidance that outlines responsibilities and processes for software application rationalization within their Components. The policy should also require DoD Components to regularly, at least annually, validate the accuracy of their owned and in use software applications inventory.

c. Conduct periodic reviews to ensure DoD Components are regularly validating the accuracy of their inventory of owned and in use software applications and that DoD Components are eliminating duplicate and obsolete software applications.

Management Comments Required

The DoD CIO did not provide a response to recommendations in a draft of this report; therefore, the recommendations are unresolved. We request that the DoD CIO provide comments on the final report.

Appendix

Scope and Methodology

We conducted this performance audit from February 2018 through November 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 objective.

We interviewed officials from the Offices of the DoD CIO and the CMO and the CIO offices of the Marine Corps, the Navy, and the Air Force responsible for managing information technology portfolios to understand the processes used to rationalize software applications and manage software licensing, and the systems used to budget information technology requirements.

We reviewed Federal laws and DoD policies, including DON and Air Force guidance, to understand the requirements for identifying and eliminating duplicative and obsolete software applications, managing software licenses, and budgeting information technology. We nonstatistically selected and visited the following Service Components.

- Marine Corps Command, Control, Communications, and Computers Network Plans and Policy Division; Washington, D.C.
- Marine Corps Logistics Plans, Policy, and Strategic Mobility Division; Washington, D.C.
- USFF; Norfolk, Virginia
- NAVSEA; Washington, D.C.
- NAVFAC; Washington, D.C.
- Headquarters Air Force CIO Support Division; Washington, D.C.
- Air Force Materiel Command; Wright-Patterson Air Force Base, Ohio

Use of Computer-Processed Data

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

Use of Technical Assistance

We consulted with the DoD OIG Quantitative Methods Division to select a nonstatistical sample of DON and Air Force commands and divisions to review. We nonstatistically selected our sample from the universe of 29 DON and Air Force commands and divisions by using the budget information related to dollar amounts from the FY 2019 President's information technology budget and data from the DoD Information Technology Portfolio Repository system to identify system identification codes. We calculated the percentage change from FY 2017 executed dollar amounts to FY 2018 budgeted amounts and nonstatistically selected a sample of five Navy and Air Force commands and divisions from the universe based on budget increase from FY 2017 to FY 2018 and location. The Marine Corps does not report their budget by division, so we coordinated with the Marine Corps to nonstatistically select two Marine Corps divisions to review.

Prior Coverage

During the last 5 years, the GAO and the Army Audit Agency issued three reports discussing information technology portfolio management, software application rationalization, and software license management. Unrestricted GAO reports can be accessed at http://www.gao.gov, and unrestricted Army Audit Agency reports can be accessed at http://www.aaa.army.mil.

GAO

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

> The GAO found that most of the 24 agencies reviewed under the Chief Financial Officers Act of 1990 fully met at least three of the four practices that GAO identified to determine if agencies had complete software application inventories. Specifically, the GAO determined that the Departments of Defense, Homeland Security, and Justice, and the General Services Administration fully met all four practices; nine agencies fully met three practices; six agencies fully met two practices; two agencies fully met one practice; and three agencies did not fully meet any practice.

Report No. GAO-14-413, "Federal Software Licenses: Better Management Needed to Achieve Significant Savings Government-Wide," May 22, 2014

The GAO found that OMB and the majority of agencies it reviewed did not have adequate policies for managing software licenses. GAO found that the DoD established policies including the establishment of a comprehensive inventory of software licenses and the analysis of these data to inform investment decisions to identify opportunities to reduce costs, but the DoD has not developed policies on centralizing management or tracking its inventory using automated tools.

Army Audit Agency

Report No. A-2017-0099-IET, "Army Data Center Closure Reports," September 28, 2017

The Army Audit Agency found that although the Army CIO made progress in collecting information on efficiencies from data center closures, the office has more work to do in refining guidance to address continuing closure report challenges. In addition, the Army Audit Agency found that Army activities identified their inventory of software applications, results of software application rationalization, equipment dispositions, contracts, and fund accounting codes. The Army Audit Agency made a recommendation to the Army CIO related to the reporting of cost savings associated with software application rationalization for data centers.

Acronyms and Abbreviations

CIO	Chief Information Officer
CMO	Chief Management Officer
COTS	Commercial Off-the-Shelf
DADMS	Department of Navy Application Database Management System
DON	Department of Navy
FAM	Functional Area Manager
FITARA	Federal Information Technology Acquisition Reform Act
NAVSEA	Naval Sea Systems Command
NAVFAC	Naval Facilities Engineering Command
OMB	Office of Management and Budget
SAF	Secretary of the Air Force
SAF/CIO A6	Chief, Information Dominance and CIO
USFF	U.S. Fleet Forces Command

Glossary

Commercial Off-The-Shelf (COTS) Software. Software that is ready-made by commercial vendors and available for sale, lease, or license to the public, as well as to the U.S. Government.

DoD Joint Information Environment. Initiative to increase cybersecurity and gain information technology efficiencies.

DON Application and Database Management System (DADMS). Web enabled registry of the Marine Corps and Navy applications and their associated data structures and the authoritative data source for information technology applications and database portfolio management.

Government Off-The-Shelf Software. Government-produced applications and COTS software that has been modified to provide the Government a specific capability and is retained and maintained inside the U.S. Government.

Information Technology Portfolio. Group of information technology investments aligned by capability to accomplish a specific functional goal, objective, or mission outcome.

Open Source Software. Software that is available in source code form, which allows code level modification and customization by vendors or programs for specific uses.

Portfolio Stat. Quarterly review of federal agencies portfolio management conducted by the agency CIOs and senior agency officials.

Software Application. A program that performs a specific function for a user, such as office automation, e-mail, or web services.

Software Application Rationalization. Process of identifying all software applications owned and in use on the enterprise networks; determining whether existing software applications are needed, duplicative, or obsolete; taking appropriate action to keep or eliminate a software application; and determining whether a software application already exists within the enterprise before purchasing an application.

Whistleblower Protection
U.S. Department of Defense

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

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

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

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

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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