Report No. DODIG-2017-073

~~FOR OFFICIAL USE ONLY~~

INSPECTOR GENERAL

U.S. Department of Defense

APRIL 7, 2017

Defense Information Systems Agency Officials Complied With Federal and DoD Policies for Managing the Defense Collaboration Services but Need to Obtain a Full Authorization to Operate

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

~~FOR OFFICIAL USE ONLY~~

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.

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

Results in Brief

Defense Information Systems Agency Officials Complied With Federal and DoD Policies for Managing the Defense Collaboration Services but Need to Obtain a Full Authorization to Operate

April 7, 2017

Objective

We determined whether the Defense Information Systems Agency (DISA) complied with Federal and DoD mandatory processes for software life cycle management of the Defense Collaboration Services (DCS).[1] Specifically, we addressed Defense Hotline allegations by determining whether DISA was effectively following Federal and DoD policies and procedures for defining software development requirements, using open source software, performing software testing, and ensuring software security.

Background

The Defense Hotline received allegations stating that DISA failed to comply with Federal and DoD processes for software management. The allegations focused on the DCS and outlined concerns of potential software security vulnerabilities. The allegations included concerns that DISA officials were not following Federal and DoD policy for defining software development requirements, using open source software, performing software testing, and ensuring software security.

Finding

We did not substantiate the Defense Hotline allegations related to inadequate software development requirements, lack of adherence to DoD Chief Information Officer direction for open source software use, and inadequate software testing and security. DISA officials complied with Federal and DoD guidance for management of the DCS. Specifically, DISA officials:

- defined software development requirements based on technical needs;
- performed code reviews for open source software and completed other actions in accordance with DoD Chief Information Officer best practices; and
- established software management processes, performed operational software testing, and ensured software security.

Although we did not substantiate the Defense Hotline allegations, we determined that the authorizing official granted DISA a 1-year authorization to operate (ATO) instead of a full 3-year ATO in May 2016.[2] The authorizing official grants the ATO based on the level of risk to organizational operations. If overall risk is determined to be acceptable, and there are no noncompliant controls with a high or very high level of risk,[3] a 3-year ATO can be granted. If overall risk is determined to be acceptable due to mission criticality, but there are noncompliant controls with a high or very high level of risk, a 1-year ATO with conditions can be granted by the authorizing official with permission of the responsible Component Chief Information Officer. After the 1-year period, if noncompliant controls with a high or very high level of risk still exist, the authorizing official may again grant a 1-year ATO with conditions only if the Component

[1] The DCS is a communication platform for the armed services which allows for worldwide collaboration on the DoD's nonclassified and secret networks by offering web conference and chat capabilities.

[2] The authorizing official is responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture. The authorizing official for the DCS is the DISA Chief of Cybersecurity.

[3] During the ATO process, the DISA Certification and Assessments Division reviews the system's information assurance controls to determine whether the controls are compliant with the risk management framework, which is DoD's integrated enterprise-wide structure for cybersecurity risk management.

Results in Brief

Defense Information Systems Agency Officials Complied With Federal and DoD Policies for Managing the Defense Collaboration Services but Need to Obtain a Full Authorization to Operate

Finding (cont'd)

Chief Information Officer grants permission. If the risk for the high or very high noncompliant controls is mitigated to an acceptable risk level, a full 3-year ATO can be granted.

DISA needs to mitigate the level of risk for high and very high noncompliant controls and obtain a 3-year ATO for the DCS. Mitigating the level of risk for these noncompliant controls will improve security of the DCS and further decrease the risk of unauthorized access.

Recommendation

We recommend that the Chief Information Officer, DISA, mitigate the level of risk for high and very high noncompliant controls identified in the May 2016 ATO to be granted a 3-year ATO for the DCS.

Management Actions Taken

We provided a discussion draft with the finding and recommendation of this report to DISA on February 27, 2017. DISA agreed and had no substantive comments on the discussion draft. Therefore, we did not require a written response, and are publishing this report in final form.

During the audit, we discussed the recommendation with the DCS program manager. The DCS program manager provided a status of actions taken to mitigate the level of risk for noncompliant controls identified in the May 2016 ATO. The DCS program manager stated that the DCS program management office information assurance team and the information systems security officer mitigated the level of risk for noncompliant controls and submitted supporting documentation to the DISA Certification and Assessments Division to support the granting of a 3-year ATO by May 8, 2017.

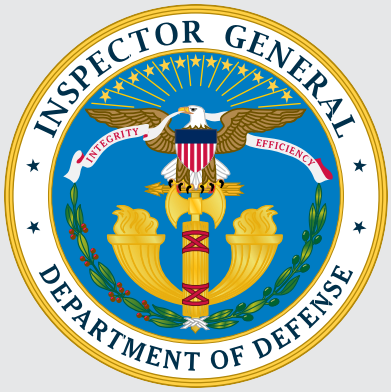
We consider the DCS program manager's response to have addressed all specifics of the recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once DISA provides us with a copy of the 2017 ATO for the DCS indicating that the level of risk for high and very high noncompliant controls were mitigated and the authorizing official granted a 3-year ATO.

Recommendation Table

Management	Recommendation Unresolved	Recommendation Resolved	Recommendation Closed
Chief Information Officer, Defense Information Systems Agency	None	1	None

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
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

April 7, 2017

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Defense Information Systems Agency Officials Complied With Federal and DoD Policies for Managing the Defense Collaboration Services but Need to Obtain a Full Authorization to Operate (Report No. DODIG-2017-073)

We are providing this report for your information and use. Defense Information Systems Agency officials complied with Federal and DoD mandatory processes for life cycle management of the Defense Collaboration Services, and we did not substantiate the relevant Defense Hotline allegations. However, we determined that the Defense Information Systems Agency did not obtain a full authorization to operate the Defense Collaboration Services, and we recommend that the Defense Information Systems Agency mitigate the level of risk for high and very high noncompliant controls and be granted a 3-year authorization to operate. We conducted this audit in accordance with generally accepted government auditing standards.

We did not issue a draft report, and no written response is required. During the audit we notified the Defense Information Systems Agency of our finding and recommendation. Defense Information Systems Agency management actions taken during the audit addressed the recommendation; therefore, the recommendation is resolved but remains open.

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

Carol N. Gorman
Assistant Inspector General
Readiness and Cyber Operations

Contents

Introduction

Objective

We determined whether the Defense Information Systems Agency (DISA) complied with Federal and DoD mandatory processes for software life cycle management of the Defense Collaboration Services (DCS). Specifically, we addressed Defense Hotline allegations by determining whether DISA effectively followed Federal and DoD policies and procedures for:

- defining software development requirements,
- using open source software,
- performing software testing, and
- ensuring software security.

Background

DISA is a DoD combat support agency that provides, operates, and assures command and control, information-sharing capabilities, and a globally accessible enterprise information infrastructure across the full spectrum of DoD operations. Defense Connect Online was the designated enterprise tool for worldwide collaboration. It was available to all DoD partners and allowed users to communicate and share information in a secure forum through instant messaging, low-bandwidth text chat, and audio/video web conferencing. DISA used Defense Connect Online from October 2007 to June 2015 to meet Net-Centric Enterprise Services[4] requirements for the DoD. In September 2013, DISA officials determined that the estimated budget for the Defense Connect Online exceeded the future years defense program budget; therefore, DISA decided to internally develop and host a similar application using open source software called the DCS. The DCS allows for worldwide collaboration on the DoD's nonclassified and secret networks by offering web conference and chat capabilities.

[4] The capability development document for Net-Centric Enterprise Services states that "net-centricity" is the realization of a globally interconnected network environment in which data is shared in a timely and seamless way among users, and Net-Centric Enterprise Services is the foundation for transforming the current environment to a dynamic and collaborative information sharing environment.

Hotline Allegations

The Defense Hotline received allegations in 2015 stating that DISA failed to comply with Federal and DoD processes for software management. The allegations centered on the DCS and outlined concerns of potential software security vulnerabilities that could endanger the warfighter by allowing foreign intelligence and terrorists to gain access to the DCS and potentially classified information. The allegations included concerns that DISA officials were not following procedures or applying standards in Federal and DoD policy for managing the software life cycle of the DCS, which included defining software development requirements, using open source software, and performing software testing and security.

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.[5] DISA internal controls were effective as they applied to the audit objective.

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

Finding

Defense Information Systems Agency Officials Complied With Federal and DoD Guidance for Managing the Defense Collaboration Services

We did not substantiate the Defense Hotline allegations related to inadequate software development requirements, lack of adherence to DoD Chief Information Officer direction for open software use, and inadequate software testing and security. DISA officials complied with Federal and DoD guidance for life cycle management of the DCS. Specifically, DISA officials defined software development requirements and performed a detailed analysis of alternatives for software solutions to replace Defense Connect Online in accordance with Federal and DoD guidance. DISA officials also performed code reviews for open source software and completed other actions in accordance with DoD Chief Information Officer best practices. Additionally, DISA officials established software management processes, performed operational software testing, and ensured software security in accordance with Federal and DoD guidance.

Although we did not substantiate the Defense Hotline allegations, we determined that the authorizing official[6] granted DISA a 1-year authorization to operate (ATO) instead of a full 3-year ATO in May 2016. The authorizing official did not grant a 3-year ATO because he identified noncompliant controls with a high and very high level of risk[7] that he required DISA to mitigate to an acceptable level of risk before he would grant a full 3-year ATO. DISA needs to mitigate the level of risk for the high and very high noncompliant controls and obtain a 3-year ATO for the DCS. Mitigating the level of risk for these noncompliant controls will improve security of the DCS and further decrease the risk of unauthorized access.

[6] The authorizing official is responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture. The authorizing official for the DCS is the DISA Chief of Cybersecurity.

[7] During the ATO process, the DISA Certification and Assessments Division reviews the system's information assurance controls to determine whether the controls are compliant with the risk management framework, which is DoD's integrated enterprise-wide structure for cybersecurity risk management.

Defense Hotline Allegations Were Not Substantiated

The Defense Hotline received allegations in 2015 related to mismanagement at DISA concerning software development and management of the DCS. We identified four Defense Hotline allegations specific to DISA's software management of the DCS. We did not substantiate any of the allegations during the audit.

Hotline Allegation 1: Mandatory Software Development Processes Not Followed

DISA failed to comply with Federal regulations and other software development standards for the DCS.

DoD OIG Response

The allegation was unsubstantiated. DISA complied with Federal Acquisition Regulation part 11 and the requirements in DoD Instruction 5000.02. DISA officials used a valid capability development document for the program and completed the required analysis of alternatives for developing the DCS as a replacement for Defense Connect Online. The analysis of alternatives identified that DISA officials conducted research, identified requirements, and planned for sustainment.

DISA Complied With Software Development Requirements

DISA officials identified valid requirements, modified requirements as needed, and performed a detailed analysis of alternatives. Federal Acquisition Regulation part 11 states that when describing agency needs, the agency is required to state, define, and modify (as needed) requirements; perform market research; and consider sustainability.[8] DoD Instruction 5000.02 requires that officials use a validated initial requirement document (or equivalent requirement document) and complete an analysis of alternatives.[9] During software development, DISA's internal policies and procedures[10] required them to clearly define, prioritize, and approve requirements.

[8] Federal Acquisition Regulation Part 11, "Describing Agency Needs," 11.000, "Scope of Part," And 11.002, "Policy."

[9] DoD Instruction 5000.02, "Operation of the Defense Acquisition System," Section 5 "Procedures," Subsection d, "Acquisition Process Decision Points and Phase Content," January 7, 2015.

[10] DISA Requirements and Analysis Process, April 16, 2016; DISA Instruction 610-225-2, "Acquisition Oversight and Management," February 19, 2015; DISA Information Technology Acquisition Guidebook, November 1, 2013; Component Acquisition Executive Guideline 004, "Projects," April 28, 2011; and Component Acquisition Executive Guideline 005, "Acquisition Review Boards," November 10, 2015.

As required by DoD Instruction 5000.02,[11] DISA officials used a valid capability development document for the DCS requirements, which the Joint Requirement Oversight Council approved on May 22, 2006.[12] DISA developed the DCS with the approved requirements and modified the requirements throughout the acquisition process based on direction from the Joint Interoperability Test Command and DoD Chief Information Officer. On March 30, 2015, DISA officials met with the DoD Chief Information Officer, who shared concerns about the DCS's video performance capabilities and the ability to add users to DCS web conferences. In November 2015, DISA officials modified the DCS to address the DoD Chief Information Officer's concerns. We verified that the DCS allowed multiple users to perform a high-quality video web conference.

As required by DoD Instruction 5000.02, DISA officials used a valid capability development document for the DCS requirements.

DISA officials conducted market research and the required analysis of alternatives and provided the analysis to the Acquisition Review Board to determine the best approach for replacing the expiring contract for Defense Connect Online. The analysis identified the following alternatives:

- re-compete Defense Connect Online services,
- focus on the development of unified capabilities as a service,
- use open source collaboration, or
- use enhanced Enterprise Voice over Internet Protocol.

The completed analysis of alternatives included cost estimates, scheduling, risk analysis, performance measurements, affordability, and capability gaps for each alternative. As a result of the analysis, DISA proceeded to complete software reviews on all open source software.

[11] DoD Instruction 5000.02 Section 5, Subsection b, "Relationship Between Defense Acquisition, Requirements, and Budgeting Processes," January 7, 2015.

[12] The Joint Requirements Oversight Council helps the Chairman of the Joint Chiefs of Staff identify and assess the priority of joint military requirements, considers alternatives to any acquisition program, and assigns priority among military programs.

Hotline Allegation 2: Outdated Open Source Software Processes

DISA failed to comply with standards or develop an actual governance process for the DCS open source software.

DoD OIG Response

The allegation was unsubstantiated. DISA officials completed required code reviews to identify vulnerabilities within the DCS open source software. DISA officials used and complied with the lessons learned and best practices for military software for open technology development, which were developed by the Assistant Secretary of Defense (Networks and Information Integration); DoD Chief Information Officer; and Under Secretary of Defense for Acquisition, Technology, and Logistics. Additionally, DISA officials set up a "benevolent dictator" governance process, and the DCS program manager established himself as the benevolent dictator.[13]

DISA Complied With DoD Open Source Software Policies

DISA officials performed code reviews in accordance with DoD Chief Information Officer best practices.[14] DISA officials also ensured that management of the DCS aligned with guidance and best practices. DISA officials adopted a governance process in compliance with the best practices.

DISA officials also ensured that management of the DCS aligned with guidance and best practices.

The DoD Chief Information Officer best practices state that open source software should have code reviews. DISA officials conducted one dynamic and two static software code reviews between March 17, 2016, and April 13, 2016.[15] DISA conducted the code reviews to evaluate the standards of source code implementation required to protect the DCS and ensure that the proper safeguards were identified, designed, and implemented within the code. The dynamic and static analysis of the DCS source code revealed vulnerabilities. We reviewed the DCS certification recommendation package, which contained actions DISA officials took to mitigate the identified vulnerabilities to a reasonable level of risk. The certification recommendation included a request for

[13] DoD Chief Information Officer's "Open Technology Development Best Practices and Lessons Learned," May 5, 2011, defines the benevolent dictator as the person in charge of final decisions. In this case, the program manager was the final decision maker.

[14] DoD Chief Information Officer's "Open Technology Development Best Practices and Lessons Learned," May 5, 2011.

[15] A dynamic code review is an analysis of the software source code operating normally. A static code review is an analysis of the actual code and may not require the software source code to be operating.

a 1-year ATO with conditions to allow DISA the opportunity to complete follow-on actions.[16] In May 2016, the authorizing official accepted the recommendation and approved a 1-year ATO with conditions.

DISA ensured that the open source software used to develop the DCS met DoD guidance. The DoD Chief Information Officer best practices state that the Government should have the right to use, modify, and distribute the source code (original programming language) of the software products. We reviewed the licenses of the open source software and determined that the licenses provided the Government those rights. DISA also ensured that the source code for the DCS software was shared across the DoD through a project site that is accessible only to those with a common access card, as required by a DoD Chief Information Officer memorandum.[17]

The DoD Chief Information Officer best practices state that projects should have a governance process. According to the best practices, the governance process for each project needs to encourage collaborative development, but it must also allow the program manager to reject suggestions from those collaborators where warranted. The best practices recommend using a benevolent dictator governance model for projects, which includes an entity who understands the project details better than others and is in charge of final decisions on the project. The DCS program manager served as the benevolent dictator and certified that the DCS was ready for an operational assessment.

Hotline Allegation 3: No Software Testing Conducted

DISA failed to implement software-testing standards for the DCS.

DoD OIG Response

The allegation was unsubstantiated. DISA officials performed operational software testing in accordance with DoD guidance outlined below. Specifically, DISA officials developed a test and evaluation master plan (TEMP) and performed operational assessments to meet software-testing requirements.[18]

[16] An ATO is a DoD authorizing decision that defines the security posture of the system. If noncompliant controls with a high or very high level of risk exist that cannot be corrected or mitigated immediately, but overall system risk is determined to be acceptable due to mission criticality, then the authorization decision will be issued in the form of an ATO with conditions.

[17] DoD Chief Information Officer memorandum, "Clarifying Guidance Regarding Open Source Software (OSS)," October 16, 2009.

[18] DISA performed all testing on the nonclassified network and applied the results to the secret network.

DISA Followed Prescribed Software Testing Processes for the DCS

DISA officials developed a TEMP and operational assessments as required by DoD policy and procedures.

DISA officials developed a TEMP and operational assessments as required by DoD policy and procedures. DoD Instruction 5000.02 states that program managers will use a TEMP as the primary planning and management tool for the integrated test program.[19] In 2014, DISA developed a TEMP for the DCS that identified and described the overall structure, processes, and objectives of the DCS Test and Evaluation program. The TEMP provided a framework to generate detailed test and evaluation plans and document schedule and resource implications associated with the Test and Evaluation program.

According to the DISA Information Technology Acquisition Guide, risk assessments are performed to determine appropriate levels of testing and to tailor testing to focus on the program's highest risk areas.[20] The DISA Information Technology Acquisition Guide requires DISA to perform risk assessments to determine the appropriate level of testing. We verified that the DCS TEMP includes a system threat (risk) assessment that identified intelligence and physical threats to the DCS. The DCS TEMP also identified the critical technical parameters that DISA uses to determine whether a system is operating effectively. DISA personnel completed two operational assessments to assess the DCS for effectiveness, suitability, interoperability, and security on the Nonclassified Internet Protocol Router Network.[21] The second operational assessment, conducted in April 2015, determined that the DCS was operationally effective.

Hotline Allegation 4: Lack of Proper Security Controls

DISA failed to follow proper software security guidance or implement proper security controls for the DCS.

DoD OIG Response

The allegation was unsubstantiated. We tested the basic access control measures when accessing the unclassified DCS website. When testing access to the DCS, we were required to enter our DoD credentials and agree to the terms-of-use agreement. We were able to establish a web conference and chat successfully.

---

[19] DoD Instruction 5000.02 "Operation of the Defense Acquisition System," Enclosure 4, "Developmental Test and Evaluation," Section 5, "Developmental Test and Evaluation Planning Considerations," January 7, 2015.

[20] DISA Information Technology Acquisition Guide, Chapter IV, "Common Process Descriptions," Section 10, "Testing."

[21] According to DoD Instruction 5000.02, the operational assessment is a test event conducted before initial production units are available. The event incorporates substantial operational realism. The DCS TEMP states that the operational assessment events focused on user observations and feedback, system performance, service desk, service operations/system administration, and operational service/performance monitoring.

We determined that access controls for the DCS web conferences provided reasonable assurance to allow only authorized users access to the application. We also verified that DISA performed the required vulnerability scans and took steps to ensure that identified threats were mitigated to a reasonable level of risk. Although DISA officials implemented National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53)[22] security controls and complied with DoD Instruction 8510.01 requirements, DISA must mitigate the level of risk for outstanding high and very high noncompliant controls to obtain a full ATO.

DISA must mitigate the level of risk for outstanding high and very high noncompliant controls to obtain a full ATO.

We identified Federal and DoD guidance for software security controls. According to NIST SP 800-53, security controls focus on the safeguards and countermeasures necessary to protect information. NIST SP 800-53 provides security and privacy controls for Federal information systems and outlines processes for selecting controls to protect organizational operations, assets, and the Nation from threats. DoD Instruction 8510.01 provides guidance for the certification and accreditation process, which results in a decision of whether Federal and DoD information systems are authorized to operate and connect to Federal and DoD networks.

DISA Implemented NIST 800-53 Security Controls

DISA officials implemented security controls and completed security scans and plans in accordance with Federal and DoD policy. According to DoD Instruction 8510.01,[23] all DoD information systems must implement security controls from NIST SP 800-53. Based on the Defense Hotline allegations, we assessed how DISA implemented risk assessments,[24] access control policy,[25] and vulnerability scanning[26] security controls from NIST SP 800-53.

---

[22] NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4, April 2013, Updated January 22, 2015.

[23] DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," Section 3, "Policy," March 12, 2014, updated May 24, 2016.

[24] According to NIST SP 800-53, Revision 4, organizations should conduct a risk assessment, including the likelihood and magnitude of harm, from unauthorized access, modification, or destruction of the information system and the information it stores. Furthermore, risk assessments should take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets.

[25] According to NIST SP 800-53, Revision 4, organizations should establish policies for effective implementation of selected security controls in the access control family.

[26] According to NIST SP 800-53, Revision 4, organizations should scan for vulnerabilities in the information system and hosted applications on an organization-defined basis and when new vulnerabilities affecting the system are identified and reported. The organization employs vulnerability scanning tools and techniques that facilitate interoperability and automate parts of the vulnerability management process.

According to the DCS security plan, risk assessments should be performed during the DCS accreditation process and whenever there are significant changes to the DCS. We found that DISA was performing risk assessments during the certification and accreditation process. We also reviewed a DCS security assessment report, updated November 3, 2016, which contained the status of security controls and unresolved issues.

(~~FOUO~~) The DCS TEMP access control requirements state that the DCS administrators will use public key infrastructure tokens to verify that users are valid DoD employees. [redacted] On October 21, 2016, we accessed the DCS on the Internet through the DoD Nonclassified Internet Protocol Router Network, where we successfully established a web conference and chat room.

DISA's Assured Compliance Assessment Solution and Continuous Monitoring and Risk Scoring systems reported information assurance vulnerability statuses in accordance with the DCS security plan. We verified that DISA officials ran weekly Assured Compliance Assessment Solution scans on the DCS assets and uploaded and reported results to the information assurance team, as required by the DCS security plan. The DCS security plan also requires Defense Enterprise Computing Center personnel to upload the scans and the Security Technical Implementation Guide results into the Enterprise Security Posture System. DISA used the Security Technical Implementation Guide results, Information Assurance Vulnerability Management assessments, and additional scanning tools to search for violations of security coding rules and guidelines for the DCS open source software.

We verified that DISA officials performed vulnerability scans to comply with NIST SP 800-53. DISA identified vulnerabilities from these scans in the certification and accreditation process from December 13, 2013, to May 4, 2016. We reviewed the certification recommendation package approved by the DISA Chief of the Certification and Assessment Division and determined that DISA officials mitigated identified vulnerabilities to an acceptable level of risk. In addition, DISA performed burp scans[27] that did not detect high-risk findings in 2016. Therefore, DISA officials implemented security controls and completed security scans and plans as required by Federal and DoD policy.

[27] Burp scans are used with manual testing methods to quickly identify many types of common vulnerabilities.

DISA Complied With Software Security Guidance

DISA officials followed the certification and accreditation processes in accordance with DoD Instruction 8510.01. The Instruction established the certification and accreditation process to ensure that a system's security risks are identified and evaluated before operation on DoD networks. DISA officials followed this process for the DCS from 2013, when they received the first Interim Authorization to Test, through May 2016.

According to DoD Instruction 8510.01, DoD officials must implement and validate information assurance controls for all DoD information systems. This is accomplished by developing and executing an implementation plan, validating information assurance controls, preparing a plan of action and milestones to address noncompliant controls,[28] and compiling the validation results in a scorecard to inform the Component Chief Information Officer of the status of the implementation of required information assurance controls. To comply with the Instruction, DISA officials developed:

- an implementation plan, which tracked implementation of DCS information assurance controls from 2014 through 2016;
- plans of action and milestones, where DISA initiated and tracked correction of DCS vulnerabilities from November 2013 to September 2016; and
- a scorecard, which tracked DCS information assurance controls from 2014 through November 2015.

To comply with DoD Instruction 8510.01 requirements, DISA appointed an information systems security manager for the DCS on February 1, 2016. DISA officials also developed a security assessment report, which complied with Instruction requirements for assessing security controls.

[28] A plan of action and milestones helps agencies identify, assess, prioritize, and monitor security weaknesses in programs and systems, along with the progress of corrective efforts for vulnerabilities. Agencies are required to prepare plan of action and milestones for all programs and systems in which an information technology security weakness has been found.

DISA Needed to Complete Additional Work on Security Conditions to Obtain a Full Authorization to Operate

(~~FOUO~~) Although we did not substantiate the Defense Hotline allegations, we determined that the authorizing official did not grant a full 3-year ATO for the DCS. The authorizing official identified high and very high noncompliant controls that he required DISA to mitigate to an acceptable level of risk before he would grant a full 3-year ATO. The authorizing official grants the ATO based on the level of risk to organizational operations. If overall risk is determined to be acceptable, and there are no high or very high noncompliant controls,[29] a 3-year ATO can be granted. If overall risk is determined to be acceptable due to mission criticality, but there are high or very high noncompliant controls, a 1-year ATO with conditions can be granted by the authorizing official with permission of the responsible Component Chief Information Officer. After the 1-year period, if noncompliant controls with a high or very high level of risk still exist, the authorizing official may again grant a 1-year ATO with conditions only if the Component Chief Information Officer grants permission. If the risks for the high or very high noncompliant controls have been mitigated, a full 3-year ATO can be granted. [redacted]

The authorizing official identified high and very high noncompliant controls that he required DISA to mitigate to an acceptable level of risk before he would grant a full 3-year ATO.

[redacted]

[29] During the ATO process, the DISA Certification and Assessments Division reviews the system's information assurance controls to determine whether the controls are compliant with the risk management framework.

The Chief Information Officer, DISA, should mitigate the level of risk for noncompliant controls to be granted a 3-year ATO for the DCS by May 8, 2017. Mitigating the level of risk for these noncompliant controls will improve security of the DCS and further decrease the risk of unauthorized access.

Recommendation

We recommend that the Chief Information Officer, Defense Information Systems Agency, mitigate the level of risk for high and very high noncompliant controls identified in the May 2016 authorization to operate to be granted a 3-year authorization to operate for the Defense Collaboration Services.

Management Actions Taken

During the audit, we discussed the recommendation with the DCS program manager. The DCS program manager provided a status of actions taken to mitigate the level of risk for noncompliant controls identified in the May 2016 ATO. The DCS program manager stated that the DCS program management office information assurance team and the information systems security officer mitigated the level of risk for noncompliant controls and submitted supporting documentation to the DISA Certification and Assessments Division to support the granting of a 3-year ATO.

Audit Response

We consider the DCS program manager's response to have addressed all specifics of the recommendation; therefore, the recommendation is resolved but remains open. We will close the recommendation once DISA provides us with a copy of the 2017 ATO for the DCS indicating that the level of risk for high and very high noncompliant controls were mitigated and the authorizing official granted a 3-year ATO.

Appendix

Scope and Methodology

We conducted this audit from August 2016 through April 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 criteria, obtained documentation, and interviewed DISA personnel. We conducted site visits to DISA headquarters at Fort Meade, Maryland, to obtain the documentation and hold the interviews necessary to understand the detailed development of the DCS at DISA. We also established the DCS web conferences and tested access controls for common access card users and guests.

Hotline Allegations

We identified the following four allegations related to DISA's software management of the DCS.

1. DISA failed to comply with Federal regulations and other software development standards for the DCS;
2. DISA failed to comply with standards or develop an actual governance process for the DCS open source software;
3. DISA failed to implement software testing standards for the DCS; and
4. DISA failed to follow proper software security guidance or implement proper security controls for the DCS.

Interviews and Documentation

To understand DISA's software life cycle management processes and how DISA applied those processes to the DCS, we interviewed DISA officials from the:

- DCS Program Management Office,
- Office of the Inspector General,
- Enterprise Engineering Directorate,
- Information Systems Security Manager, and
- Requirements and Analysis Office.

We obtained and analyzed the following Federal and DoD policy and guidance to determine whether DISA followed them for managing and developing the DCS.

- Federal Acquisition Regulation Part 11, "Describing Agency Needs," 11.000 and 11.002, June 15, 2016;
- NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," Revision 1, February 2010;
- NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013;
- DoD Chief Information Officer's "Open Technology Development Best Practices and Lessons Learned," May 5, 2011;
- DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013;
- DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks," November 5, 2012;
- DoD Instruction 8510.01, "Risk Management Framework for DoD Information Technology," March 12, 2014, updated May 24, 2016;
- DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process," November 28, 2007; and
- DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015.

In addition, we obtained and analyzed the 2006 Net-Centric Enterprise Services capabilities development document, the DCS TEMP, the DCS operational assessments, the DCS code review report, the DCS vulnerability assessments, the DCS security plan, the DCS contract, and software licenses.

Use of Computer-Processed Data

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

Prior Coverage

During the last 5 years, the DoD Office of Inspector General (DoD OIG) issued one report related to this audit. Unrestricted DoD OIG reports can be accessed at http://www.dodig.mil/pubs/index.cfm.

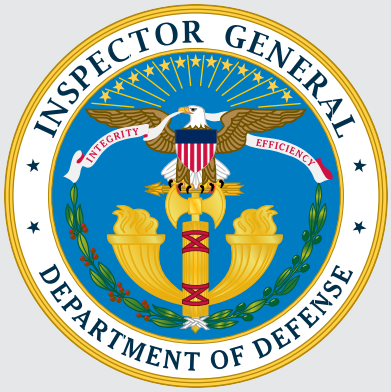
DoD OIG

Report No. DODIG-2013-107, "Defense Information Systems Agency Needs to Improve Its Information Assurance Vulnerability Management Program," July 26, 2013 (Document is FOUO)

(~~FOUO~~) [redacted]

Acronyms and Abbreviations

ATO	Authorization to Operate
DCS	Defense Collaboration Services
DISA	Defense Information Systems Agency
NIST	National Institute of Standards and Technology
SP	Special Publication
TEMP	Test and Evaluation Master Plan


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit 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
http://www.dodig.mil/pubs/email_update.cfm

Twitter
twitter.com/DoD_IG

DoD Hotline
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