U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S DEVELOPMENT TEST PRODUCTION GENERAL SUPPORT SYSTEM FY 2014

Report No. 4A-CI-00-14-015

Date: June 6, 2014

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S DEVELOPMENT TEST PRODUCTION GENERAL SUPPORT SYSTEM FY 2014

WASHINGTON, D.C.

Report No. 4A-CI-00-14-015

Date: June 6, 2014

Michael R. Esser
Assistant Inspector General for Audits

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S DEVELOPMENT TEST PRODUCTION GENERAL SUPPORT SYSTEM FY 2014

WASHINGTON, D.C.

Report No. 4A-CI-00-14-015

Date: June 6, 2014

This final audit report discusses the results of our audit of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Development Test Production General Support System (DTP). Our conclusions are detailed in the "Results" section of this report.

Security Assessment and Authorization (SA&A)

DTP does not have a current SA&A package, nor an active authorization to operate.

Federal Information Processing Standards (FIPS) 199 Analysis

A FIPS199 analysis was last performed on DTP as a part of the 2010 SA&A package that expired in August 2013.

System Security Plan (SSP)

A SSP was last developed for DTP as a part of the 2010 SA&A that expired in August 2013.

Risk Assessment

A risk assessment was last conducted for DTP as a part of the 2010 SA&A that expired in August 2013.

Independent Security Control Testing

Security controls were not independently assessed for DTP within the past three years, as required by National Institute of Standards and Technology (NIST) and OPM policy.

Security Control Continuous Monitoring

The owners of DTP did not submit continuous monitoring security reports in March or September, 2013, as required by OPM policy. However, a report has been submitted in April 2014.

Contingency Planning and Contingency Plan Testing

A contingency plan was developed for DTP that is in compliance with NIST, however the contingency plan for DTP has not been tested in the past year.

Privacy Impact Assessment (PIA)

A privacy threshold analysis was conducted for DTP that determined that a PIA was not required.

Plan of Action and Milestones (POA&M) Process

The DTP POA&M follows the format of the OPM POA&M guide, and has been routinely submitted to the OCIO for evaluation.

NIST Special Publication 800-53 Revision 4 Evaluation

We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 4 was implemented for DTP. We determined that one area of controls related to the change management process could be improved.

System Organization and Classification

The production environment of DTP resides on OPM's Local Area Network/Wide Area Network (LAN/WAN) General Support System, and is not segregated from the production applications hosted on LAN/WAN. Essentially there are two production environments.

While there are clearly defined technical boundaries segregating the development and test environments from the production environment within DTP, there should only be one production environment in OPM's infrastructure.

Contents

Introduction

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107‑347), which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we audited the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Development Test Production General Support System (DTP).

Background

The DTP environment is a general support system that was designed to be a separate technical environment from OPM's Local Area Network / Wide Area Network (LAN/WAN) production environment. DTP is intended to host the testing and development of applications, while LAN/WAN is designed to hose production applications.

Objectives

Our objective was to perform an evaluation of the security controls for DTP to ensure that the Office of the Chief Information Officer (OCIO) has implemented IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual and OPM's OCIO.

The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for DTP, including:

- Security Assessment and Authorization;
- FIPS 199 Analysis;
- System Security Plan;
- Risk Assessment;
- Independent Security Control Testing;
- Security Control Continuous Monitoring;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and
- NIST Special Publication 800-53 Revision 4 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of the OCIO, including IT security controls in place as of March 2014.

We considered the DTP internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives.

To accomplish our objectives, we interviewed OPM personnel with security responsibilities for DTP. We reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of DTP are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the DTP system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Handbook;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- The Federal Information System Controls Audit Manual;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
- Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from October 2013 through March 2014 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding DTP.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OCIO's management of DTP is consistent with applicable standards. Nothing came to our attention during this review to indicate that the OCIO is in violation of relevant laws and regulations.

Results

I. Security Assessment and Authorization

DTP does not have a current Security Assessment and Authorization (SA&A) package, nor an active authorization to operate.

The most recent SA&A of DTP was completed in August 2010, and expired in August 2013.

NIST SP 800-37 Guide for the Security Certification and Accreditation of Federal Information Systems, provides guidance to federal agencies in meeting security accreditation requirements. Although the 2010 SA&A is no longer valid, it appears to have been conducted in compliance with NIST requirements.

Recommendation 1

We recommend that the DTP environment be subject to a complete and current SA&A process.

OCIO Response:

"OCIO intends to make the DTP environment a sub-system of the LAN/WAN GSS within the next four months. The LAN/WAN GSS will have a new SA&A completed at that time. Many of the weaknesses identified within this OIG audit with the DTP environment will be remediated as a result of that SA&A process."

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide OPM's Internal Oversight and Compliance (IOC) division with evidence that DTP has been migrated under the LAN/WAN as a sub-system. Furthermore, the OCIO should provide IOC with an updated LAN/WAN System Security Plan that includes DTP as a minor application and documents the security controls that DTP inherits from the LAN/WAN.

II. FIPS 199 Analysis

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires federal agencies to categorize all federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels.

NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories, provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

The OCIO leveraged FIPS 199 to analyze the information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. As of June 24, 2010 DTP is categorized with a low impact level for confidentiality and availability, and a moderate impact level for integrity, resulting in an overall categorization of moderate.

The security categorization of DTP appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and the OIG agrees with the categorization of moderate.

However, the most recent FIPS 199 analysis performed on DTP was part of the previous SA&A package that, as mentioned in section I above, expired in August 2013.

III. System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in a SSP for each system, and provides guidance for doing so.

The SSP for DTP contains the majority of the elements outlined in NIST SP 800-18.

However, the most recent SSP developed for DTP was part of the previous SA&A package that, as mentioned in section I above, expired in August 2013.

IV. Risk Assessment

A risk assessment is used as a tool to identify security threats, vulnerabilities, potential impacts, and probability of occurrence. In addition, a risk assessment is used to evaluate the effectiveness of security policies and recommend countermeasures to ensure adequate protection of information technology resources.

NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, offers a nine step systematic approach to conducting a risk assessment that includes: (1) system characterization; (2) threat identification; (3) vulnerability identification; (4) control analysis; (5) likelihood determination; (6) impact analysis; (7) risk determination; (8) control recommendation; and (9) results documentation.

A risk assessment was conducted for DTP as a part of its 2010 SA&A that addressed all major elements outlined in the NIST guidance.

However, the most recent risk assessment performed on DTP was part of the previous SA&A package that, as mentioned in section I above, expired in August 2013.

V. Independent Security Control Testing

An independent security control assessment was completed for DTP in August 2010 as a part of the system's SA&A process. The security assessment was conducted by another government entity, the Bureau of Public Debt. We reviewed the documentation resulting from this test to ensure that it included a review of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

Independent security control testing is part of the SA&A process and should be performed at least every three years. DTP was due for independent security control testing in August 2013.

VI. Security Control Continuous Monitoring

FISMA requires that the IT security controls of each major application owned by a federal agency be tested on an annual basis. Furthermore, NIST SP 800-53 Revision 4 mandates the development of a security assessment plan and outlines the required inclusions.

The most recent self-assessment of security controls for DTP was conducted in August 2012. All major elements outlined in the NIST guidance were addressed.

OPM's internal IT policies now require that the IT security controls of each major application owned by a federal agency be tested on a continual basis. In the years that an independent assessment is not being conducted as part of an SA&A, the system's owner must test a subset of security controls twice per year in accordance with OPM's continuous monitoring methodology.

The owners of DTP did not submit continuous monitoring security reports in March or September, 2013, as required by OPM policy.

Recommendation 2

We recommend that DTP be subject to continuous monitoring of security controls in accordance with OPM policy.

OCIO Response:

"OCIO completed and submitted the Information System Continuous Monitoring Report for the DTP environment on 04/16/14. This report encompassed all the moderate controls that ITSP required to be tested in Q1 and Q2 of FY14."

OIG Reply:

The evidence provided by the OCIO in response to the draft audit report indicates that the FY 2014 quarter two continuous monitoring submission was in compliance with OPM requirements. As part of the audit resolution process, we recommend that OCIO provide OPM's IOC division with evidence of the next continuous monitoring submission.

VII. Contingency Planning and Contingency Plan Testing

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The DTP contingency plan documents the functions, operations, and resources necessary to restore and resume DTP operations when unexpected events or disasters occur. The DTP

contingency plan follows the format suggested by NIST SP 800-34 Revision 1 and contains a majority of the suggested elements.

Contingency Plan Test

NIST SP 800-34 Revision 1 also provides guidance for testing contingency plans and documenting the results. In addition, NIST SP 800-53 Revision 4, control CP-3, requires system owners to "train personnel in their contingency roles and responsibilities to the information system and provide refresher training."

The contingency plan for DTP has not been tested in the past year.

Recommendation 3

We recommend that the owners of DTP test the system's contingency plan annually.

OCIO Response:

"OCIO agrees that the DTP contingency plan has not been tested. OCIO is currently in the process of updating and testing the LAN/WAN GSS Contingency Plan. DTP will collapse in to the LAN/WAN GSS at which point the LAN/WAN contingency plan will encompass DTP."

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide OPM's IOC division with evidence that the DTP contingency plan was tested as a part of the annual LAN/WAN contingency plan test.

VIII. Privacy Impact Assessment

FISMA requires agencies to perform a screening of federal information systems to determine if a Privacy Impact Assessment (PIA) is required for that system. OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate any vulnerabilities of privacy in information systems and to document any privacy issues that have been identified and addressed. The OPM Privacy Impact Assessment Guide states that "all OPM IT systems must have a Privacy Threshold Analysis (PTA) which is utilized to determine if a PIA is required."

The OCIO completed a PTA of DTP and determined that a PIA was not required for this system.

IX. Plan of Action and Milestones Process

A Plan of Action and Milestones (POA&M) is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

The OIG evaluated the DTP POA&M and verified that it follows the format of OPM's standard template, and that updates are routinely submitted to the OCIO for evaluation.

We found no issues with the POA&M process for DTP.

X. NIST SP 800-53 Revision 4 Evaluation

NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated whether a subset of these controls had been adequately implemented for DTP. These controls were evaluated by interviewing individuals with DTP security responsibilities, reviewing documentation and system screenshots, and viewing demonstrations of system capabilities. We determined that the controls described below could be improved.

a) CM-3 Configuration Change Control & CM-5 Access Restrictions for Change

DTP application programmers have the technical ability to develop a change and move it into production without following the appropriate change control process.

NIST SP 800-53 Revision 4 requires organizations to appropriately control changes to the information system, ensuring all changes are formally approved prior to implementation and that the change process is reviewed. Logical access restrictions must be defined, documented, approved, and enforced for all changes to the information system. The OCIO must also ensure that it "tests, validates, and documents changes to the information system before implementing the changes on the operational system."

NIST SP 800-53 Revision 4 explains that "any changes to the . . . system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals [should be] allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications."

The size of the change should not justify a diversion from the approved System Development Life Cycle (SDLC). Furthermore, to ensure appropriate segregation of duties, a separate business unit should be responsible for moving code between development/test and production. No one individual should be able to migrate a change through the entire change control environment.

Recommendation 4

We recommend that the OCIO make the appropriate system modifications to ensure appropriate segregation of duties are enforced within DTP.

OCIO Response:

"OCIO agrees that the DTP system segregation of duties is not adequate. The LAN/WAN GSS is in the process of reorganizing roles and functions within the environment to ensure segregation of duties. The LAN/WAN GSS is in the process of instituting technical controls between environments which would ensure that changes are not made without following the correct protocols. DTP will be able to leverage these changes as soon as it is converted in to a subsystem of the LAN/WAN GSS."

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide OPM's IOC division with evidence that roles and responsibilities are appropriately adjusted with the reorganization of the environment to ensure proper segregation of duties.

Recommendation 5

We recommend that the OCIO make the appropriate organizational modification to ensure a business unit independent of the application developers migrates changes into production. That same business unit should be responsible for validating that all elements of the SDLC were followed, changes were appropriately tested, and all documentation is valid and approved prior to migrating changes into production.

OCIO Response:

"OCIO agrees that there are weaknesses within the SDLC process of the DTP environment. The LAN/WAN currently utilizes a change control board in order to facilitate any changes to the environment. The LAN/WAN plans to also put more stringent measures in place to ensure that the SDLC process is followed, changes are tested, and all documentation is valid prior to migration to the production environment. DTP will be able to leverage these changes as soon as it is converted in to a subsystem of the LAN/WAN GSS."

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide OPM's IOC division with evidence that changes for DTP follow the approved SDLC with regard to both procedure and documentation, and that the individuals with the technical capability to migrate changes to production are independent of the developers, testers, and business users.

b) CM-6 Configuration Settings

We conducted vulnerability scans of the databases and servers supporting DTP using AppDetective Pro and Nessus scanning tools. Although the technical details of these settings will not be included in this report, the OCIO has been provided with this information.

The vulnerability scans revealed that both the database and server generally contain settings configured in a manner compliant with OPM's configuration policies.

XI. System Organization and Classification

a) Multiple Production Environments

DTP is a general support system intended to be used for the development and testing of new and/or modified applications hosted in the LAN/WAN production environment. Currently, DTP is comprised of a development, test, and production environment. However, the production environment of DTP resides on the LAN/WAN and is not segregated from the production applications hosted on LAN/WAN. Essentially there are two production environments.

While there are clearly defined technical boundaries segregating the development and test environments from the production environment within DTP, there should only be one production environment in OPM's infrastructure.

Recommendation 6

We recommend that the OCIO make the appropriate system modification to ensure that there is only one production environment in OPM's technical infrastructure.

OCIO Response:

"OCIO agrees that there should only be one production environment. OCIO intends to convert DTP in to a subsystem of the LAN/WAN GSS within the next four months. At that point there will only be one production environment."

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide OPM's IOC division with evidence that the conversion of DTP to a subsystem of the LAN/WAN GSS results in only one production environment.

b) Reclassification of DTP

DTP is currently classified as a "major application" and is included on OPM's master inventory of major systems. During the course of the audit we were informed that it is the intention of the OCIO to reclassify the development and test elements of DTP as subsystems under the LAN/WAN, and to consolidate the production elements of DTP into the LAN/WAN production environment.

OPM's LAN/WAN general support system (also owned and operated by the OCIO) currently supports a variety of minor applications. Considering the OCIO currently provides technical support for DTP and the system already resides within the boundaries of the LAN/WAN, we believe this would be an appropriate way to address our audit concerns.

As part of the reclassification process, the OCIO should update the LAN/WAN SSP to include DTP as a minor application and to document the security controls that DTP inherits from the general support system.

Although reclassifying DTP as a minor application would alleviate some of the SA&A related requirements applicable to major systems, it does not absolve the OCIO from ensuring the remediation of the security weaknesses identified in prior security assessments and this audit report.

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Group Chief
- [redacted], Lead IT Auditor-in-Charge
- [redacted], IT Auditor

APPENDIX

United States Office of Personnel Management

U.S. Office of Personnel Management
1900 E Street, NW
Washington D.C. 20415

MEMORANDUM FOR: [redacted]
Lead IT Auditor

FROM: [redacted]
Designated Security Officer

SUBJECT: DTP Response to OIG Audit

OIG Recommendation 1
We recommend that the DTP environment be subject to a complete and current SA&A process.

OCIO Response:

OCIO intends to make the DTP environment a sub-system of the LAN/WAN GSS within the next four months. The LAN/WAN GSS will have a new SA&A completed at that time. Many of the weaknesses identified within this OIG audit with the DTP environment will be remediated as a result of that SA&A process.

OIG Recommendation 2
We recommend that DTP be subject to continuous monitoring in accordance with OPM policy.

OCIO Response:

OCIO completed and submitted the Information System Continuous Monitoring Report for the DTP environment on 04/16/14. This report encompassed all the moderate controls that ITSP required to be tested in Q1 and Q2 of FY14.

Recommendation 3
We recommend that the owners of DTP test the system's contingency plan.

OCIO Response:

OCIO agrees that the DTP contingency plan has not been tested. OCIO is currently in the process of updating and testing the LAN/WAN GSS Contingency Plan. DTP will collapse in to the LAN/WAN GSS at which point the LAN/WAN contingency plan will encompass DTP.

Recommendation 4
We recommend that the OCIO make the appropriate system modifications to ensure appropriate segregation of duties are enforced within DTP.

OCIO Response:

OCIO agrees that the DTP system segregation of duties is not adequate. The LAN/WAN GSS is in the process of reorganizing roles and functions within the environment to ensure segregation of duties. The LAN/WAN GSS is in the process of instituting technical controls between environments which would ensure that changes are not made without following the correct protocols. DTP will be able to leverage these changes as soon as it is converted in to a subsystem of the LAN/WAN GSS.

Recommendation 5
We recommend that the OCIO make the appropriate organizational modification to ensure a business unit independent of the change process migrates changes into production. That same business unit should be responsible for validating that all elements of the SDLC were followed, changes were appropriately tested, all documentation is valid and approved prior to migrating changes into production.

OCIO Response:

OCIO agrees that there are weaknesses within the SDLC process of the DTP environment. The LAN/WAN currently utilizes a change control board in order to facilitate any changes to the environment. The LAN/WAN plans to also put more stringent measures in place to ensure that the SDLC process is followed, changes are tested, and all documentation is valid prior to migration to the production environment. DTP will be able to leverage these changes as soon as it is converted in to a subsystem of the LAN/WAN GSS.

Recommendation 6
We recommend that the OCIO make the appropriate system modification to ensure that there is only one production environment.

OCIO Response:

OCIO agrees that there should only be one production environment. OCIO intends to convert DTP in to a subsystem of the LAN/WAN GSS within the next four months. At that point there will only be one production environment.

[redacted], Designated Security Officer

5-20-14
Date