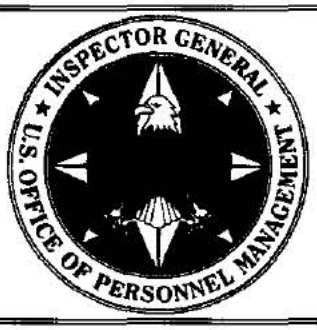

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S Center for Talent Services General Support System FY 2011

Report No. 4A-CI-00-11-043

Date: 9/28/11

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S CENTER FOR TALENT SERVICES GENERAL SUPPORT SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-CI-00-11-043

Date: 9/28/11

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S CENTER FOR TALENT SERVICES GENERAL SUPPORT SYSTEM FY 2011

WASHINGTON, D.C.

Report No. 4A-CI-00-11-043

Date: 9/28/11

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) Center for Talent Services General Support System (CTS GSS). Our conclusions are detailed in the "Results" section of this report.

Certification and Accreditation (C&A)

A security C&A of CTS GSS was completed in July 2009. We reviewed the certification package for all required elements of a C&A, and determined that the package contained all necessary documentation.

Federal Information Processing Standards (FIPS) 199

A FIPS 199 Analysis of CTS GSS was conducted in May 2009. We agree with the security categorization of moderate for CTS GSS.

Information System Security Plan (ISSP)

The ISSP for CTS GSS contains the critical elements required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18.

Risk Assessment

A risk assessment was conducted for CTS GSS in August 2010 that addresses all the required elements outlined in relevant NIST guidance.

Independent Security Test and Evaluation (ST&E)

An independent ST&E was completed for CTS GSS as a part of the system's C&A process in May 2009.

Annual Self-Assessment

HRS conducted a thorough self-assessment of the security controls of CTS GSS in June 2010.

Contingency Plan

A contingency plan was developed for the CTS GSS that is in compliance with NIST SP 800-34. However, the CTS GSS contingency plan has only been tested using tabletop exercises instead of the functional exercise that is required in NIST SP 800-84.

Privacy Impact Assessment (PIA)

A privacy threshold analysis (PTA) was conducted for the CTS GSS. The PTA revealed that CTS GSS does not require a PIA; we agree with this assessment.

Plan of Action and Milestones (POA&M)

The CTS GSS POA&M follows the format of the OPM POA&M guide, and has been routinely submitted to the Office of the Chief Information Officer for evaluation.

NIST SP 800-53 Evaluation

We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 were implemented for CTS GSS. Although the majority of the tested security controls have been successfully implemented, several controls were not fully satisfied, including:

- The computer room that houses the CTS GSS does not have an automatic fire suppression system as recommended in NIST SP 800-53.
- HRS does not have documented emergency response procedures or conduct annual emergency response training as required in NIST SP 800-53.

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) Center for Talent Services General Support System (CTS GSS).

Background

CTS GSS is one of OPM's critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's systems on a rotating basis.

CTS GSS provides design, development, and operation of human resources systems for a variety of functions and customers across the government. OPM's Human Resources Solutions (HRS) is the organization responsible for the software development, maintenance, and operations of the systems contained within the CTS GSS. The hardware supporting those systems is housed at OPM's Macon, Georgia facility.

This was our first audit of the security controls surrounding CTS GSS. We discussed the results of our audit with HRS representatives at an exit conference.

Objectives

Our objective was to perform an evaluation of the security controls for CTS GSS to ensure that HRS officials have 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 (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

OPM's IT security policies require managers of all major information systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for CTS GSS, including:

- Certification and Accreditation Statement;
- FIPS 199 Analysis;
- Information System Security Plan;
- Risk Assessment;
- Independent Security Control Testing;
- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;

- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53 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 HRS officials responsible for CTS GSS, including IT security controls in place as of May 2011.

We considered the CTS GSS 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 objective, we interviewed representatives of OPM's HRS division and other individuals with CTS GSS security responsibilities. 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 CTS GSS 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 CTS GSS system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy Volumes 1 and 2;
- 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, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;
- 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 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 March 2011 through May 2011 in OPM's Washington, D.C. and Macon, Georgia offices. This was our first audit of the security controls surrounding CTS GSS.

Compliance with Laws and Regulations

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

Results

I. Certification and Accreditation Statement

A security certification and accreditation (C&A) of the CTS GSS was completed in July 2009.

OPM's Acting IT Security Officer (representing the Office of the Chief Information Officer or OCIO) reviewed the CTS GSS C&A package and signed the system's certification package on July 7, 2009. The system's owner signed the accreditation statement and authorized the continued operation of the system on July 13, 2009.

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. The CTS GSS C&A appears to have been conducted in compliance with NIST requirements.

OPM's OCIO created and published guidance for preparing and conducting C&A's in January 2011. These policies and procedures are now in effect for all OPM systems. While the CTS GSS C&A was appropriately conducted in accordance with the guidance available in 2009, we suggest that HRS review OPM's new C&A methodology and conduct a gap analysis to ensure that they are prepared to conduct their 2012 C&A in accordance with the new requirements.

II. Federal Information Processing Standards (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.

A FIPS 199 analysis of CTS GSS was conducted in May 2009 as part of the system's Information System Security Plan (ISSP) development. The ISSP categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. CTS GSS is categorized with a moderate impact level for confidentiality, moderate for integrity, moderate for availability, and an overall categorization of moderate.

The security categorization of CTS GSS appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and we agree with the categorization of moderate.

III. Information System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information

Systems. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in an ISSP for each system, and provides guidance for doing so.

The ISSP for CTS GSS was created using the template outlined in NIST SP 800-18. The template requires that the following elements be documented within the ISSP:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

The CTS GSS ISSP adequately addresses each of the elements required by NIST.

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, Risk Management Guide for Information Technology Systems, 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 CTS GSS in August 2010 that adequately addresses all of the elements outlined in the NIST guidance.

V. Independent Security Control Testing

A Security Test and Evaluation (ST&E) was completed for CTS GSS in May 2009 as a part of the system's C&A process. The ST&E was conducted by a contractor, Network Security Systems Plus Inc., which was operating independently from HRS. We reviewed the controls within the scope of this test to ensure that they 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 3, Recommended Security Controls for Federal Information Systems.

The ST&E report labeled each security control as fully satisfied, partially satisfied, not satisfied, not verified, or not applicable. Several controls were also identified as controls inherited from OPM's [redacted] Nothing came to our attention to indicate that the security controls of CTS GSS have not been adequately tested by an independent source.

VI. Security Control Self-Assessment

FISMA requires that the IT security controls of each major application owned by a federal agency be tested on an annual basis. In the years that an independent ST&E is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls.

HRS conducted a self-assessment of the system in June 2010. The assessment included a review of the relevant management, operational, and technical security controls outlined in NIST SP 800-53 Revision 3. Nothing came to our attention to indicate that the security controls of CTS GSS have not been adequately tested by HRS.

VII. Contingency Planning and Contingency Plan Testing

NIST SP 800-34, Contingency Planning Guide for Information Technology 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 CTS GSS contingency plan documents the functions, operations, and resources necessary to restore and resume CTS GSS operations when unexpected events or disasters occur. The CTS GSS contingency plan closely follows the format suggested by NIST SP 800-34 and is compliant with the required elements of the guidance.

Contingency Plan Test

NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A simulated "table top" test of the CTS GSS contingency plan was conducted by HRS officials in April 2010. The simulation test involved reviewing a series of steps that must be completed to recover the system in a predetermined disaster situation. The testing documentation contained an analysis and review of the simulation results. We reviewed the testing documentation to determine if the test conformed with NIST 800-34 guidelines.

While HRS conducts annual table top tests of the contingency plan, they have never performed a functional disaster recovery exercise. A functional exercise would allow HRS to further validate their readiness for disruptive events by performing system restoration activities in an operational environment. Since CTS GSS is a general support system that houses five major OPM systems and eight minor systems, we believe that a functional exercise to test the contingency plan should be conducted annually.

NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Section 5.1, states that "Organizations should conduct functional exercises periodically; following organizational changes, updates to an IT plan, or the issuance of new TT&E [Test, Training, and Exercise] guidance; or as otherwise needed." Failure to conduct functional contingency plan exercises prevents HRS from discovering unanticipated technical or logistical problems or limitations that could arise while restoring the CTS GSS at the alternate location.

Recommendation 1

We recommend HRS conduct a functional contingency plan test for the CTS GSS.

HRS Response:

"HRS concurs with the recommendation and will conduct a functional contingency plan test for the CTS GSS during FY12."

OIG Reply:

As part of the audit resolution process, we recommend that HRS provide Internal Oversight and Compliance (IOC) with evidence that it has conducted a functional contingency plan test.

Recommendation 2

We recommend HRS coordinate with the system owners whose systems reside on the CTS GSS to encourage their participation in the functional contingency plan exercises.

HRS Response:

"HRS concurs with this recommendation and will coordinate the functional contingency plan test with system owners whose systems reside on the CTS GSS 60 days prior to the actual test."

OIG Reply:

As part of the audit resolution process, we recommend that the HRS provide IOC with evidence that it has coordinated with the system owners whose systems reside on the CTS GSS.

VIII. Privacy Impact Assessment (PIA)

The E-Government Act of 2002 requires agencies to perform a screening of federal information systems to determine if a 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.

HRS completed an initial privacy threshold analysis of CTS GSS and determined that a PIA was not required for this system because it does not contain Personally Identifiable Information (PII). Although several applications residing on CTS GSS servers contain PII, the HRS staff supporting CTS GSS does not have access to this data.

IX. Plan of Action and Milestones Process (POA&M)

A 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 CTS GSS POA&M and verified that it follows the format of OPM's standard template, and has been routinely submitted to OCIO for evaluation. We also determined that the POA&M contained action items for all security weaknesses identified through various security control tests and audits.

Nothing came to our attention to indicate that there are any current weaknesses in the management of the CTS GSS POA&M.

X. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated the degree to which a subset of these controls had been implemented for CTS GSS, including:

- AC-2 Account Management
- AC-5 Separation of Duties
- AC-6 Least Privilege
- AC-11 Session Lock
- AT-3 Security Training
- AT-4 Security Training Records
- AU-2 Auditable Events
- AU-6 Audit Review, Analysis, Reporting
- CA-7 Continuous Monitoring
- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- CP-3 Contingency Training
- IA-1 Identification and Authentication Policy and Procedures
- IA-2 Identification and Authentication (Organizational user)
- IA-5 Authenticator Management
- IR-2 Incident Response Training
- IR-5 Incident Monitoring
- MA-1 System Maintenance Policy and Procedures

- MA-2 Controlled Maintenance
- PL-4 Rules of Behavior
- PS-4 Personnel Termination
- RA-5 Vulnerability Scanning
- SC-5 Denial of Service Protection
- SI-2 Flaw Remediation
- PM-1 Information Security Program Plan
- MP-6 Media Sanitization and Disposal
- PE-1 through PE-18 Physical and Environmental Controls
- SA-7 User-Installed Software
- SC-13 User of Cryptography
- SI-9 Information Input Restrictions

These controls were evaluated by interviewing individuals with CTS GSS security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system.

Although it appears that the majority of NIST SP 800-53 Revision 3 security controls have been successfully implemented for the CTS GSS, several tested controls were not fully satisfied.

a) PE-13 Fire Protection

The CTS GSS computer room does not contain an automatic fire suppression system. The CTS GSS currently relies on hand-held fire extinguishers located within the computer room as their sole means of fire suppression. HRS stated that they have completed an informal cost benefit analysis and concluded it would not be cost effective to install an automated fire suppression system. The HRS Standard Operating Procedures states that the organization has accepted the risk, but no formal documentation or analysis has been created.

NIST SP 800-53 Rev. 3 requires that "The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source." One of the control enhancements for a moderate risk system such as CTS GSS requires that "The organization employs an automatic fire suppression capability for the information system when the facility is not staffed on a continuous basis." While the Macon building is staffed on a continuous basis, we observed that the computer room is often unoccupied.

Failure to implement an automatic fire suppression system increases the risk that a fire could spread within the computer room before it could be extinguished by a person. Also, it would be hazardous for a person to attempt to extinguish a fire with a handheld fire extinguisher. This would greatly affect the availability of the applications that reside on the CTS GSS.

Recommendation 3

We recommend HRS install a fire suppression system within the Macon facility's computer room.

HRS Response:

"HRS employs and maintains a Johnson Controls IFC fire detection and alarm system that is automatically activated in the event of a fire and has been duly inspected and certified. Fire detection devices/systems include hand-held and wheeled fire extinguishers, fixed fire hoses, and state-of-the-art laser smoke detectors. Having an automatic fire suppression system increases the risk of the suppression agent causing more damage to the equipment than an actual fire. There is minimal material in the room that is combustible thus reducing the potential of a fire spreading. HRTT does not currently employ automatic fire suppression devices due to cost and practicality constraints. HRTT's strategy is to monitor closely and maintain a rapid response capability to enable suppression in a surgical fashion in the event of a fire rather than broadcast a fire suppression agent and affect the entire computer room, making all systems there unreachable for an unacceptable period of time. HRTT has in place a number of countermeasures to reduce the fire risk.

- ***A Macon fire station is less than two miles away from the facility (Macon-Bibb County Fire Department is A-1 rated).***
- ***The facility is staffed 24/7 by a security guard who is a state-certified, professional law enforcement officer trained as a first responder that has access to the computer room to manually activate the fire suppression mechanisms.***
- ***Existence of a laser smoke detection system in the computer room which employs detectors that are multiple times more sensitive than normal smoke detectors and trigger automatic alarms to the security staff.***
- ***Security guards also perform physical walk-through inspection of all areas every 2 to 4 hours.***
- ***The walls and ceiling of the computer room are made of reinforced concrete and its doors are fire-resistant rated at 1200 degrees Fahrenheit for one hour.***

HRS plans to conduct a cost-benefit analysis and formal risk assessment to evaluate the costs and risks of implementing an automatic fire suppression system by the end of FY12 Quarter 2."

OIG Reply:

We continue to recommend that HRS install an automatic fire suppression system in the Macon facility's computer room. However, we would consider supporting the closure of this recommendation if HRS provides IOC with a thorough risk assessment or cost-benefit analysis clearly illustrating that the costs and risks of implementing a fire suppression system exceed the benefits. HRS would also need to provide IOC with an approved official risk acceptance document.

b) PE-1 Physical and Environmental Protection Policy and Procedure

Although the current employees at the OPM Macon facility have an informal understanding of their roles and responsibilities when responding to an emergency, HRS does not have any documented emergency response procedures and does not conduct any formal emergency response training.

NIST SP 800-53 Rev. 3 requires that an organization have "A formal, documented physical and environmental protection policy that addresses purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance" and "Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls."

Furthermore, FISCAM requires that "Staff should be trained in and aware of their responsibilities in preventing, mitigating, and responding to emergency situations… information on emergency procedures and responsibilities can be provided through training sessions and by distributing written policies and procedures."

Failure to establish documented emergency response procedures increases the likelihood that personnel will not know how to respond in emergency situations within the computer room. This issue is magnified by the fact there is no automatic fire suppression system in the computer room as stated above.

Recommendation 4

We recommend HRS document and implement formal emergency response procedures.

HRS Response:

"HRS concurs with the recommendation and will document and implement formal emergency response procedures by the end of FY12 Quarter 1."

OIG Reply:

As part of the audit resolution process, we recommend that the HRS provide IOC with evidence that it has documented and implemented formal emergency response procedures.

Recommendation 5

We recommend HRS conduct annual emergency response training.

HRS Response:

"HRS concurs with this recommendation and will conduct annual emergency response training by the end of FY12 Quarter 2."

OIG Reply:

As part of the audit resolution process, we recommend that the HRS provide IOC with evidence that it conducts annual emergency response training.

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], Senior Team Leader
- [redacted], Auditor in Charge
- [redacted], IT Auditor

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Human Resources Solutions

July 15, 2011

MEMORANDUM FOR [redacted]
Chief, Information Systems Audits Group

FROM: NANCY KICHAK
Associate Director, Human Resources Solutions

SUBJECT: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Center for Talent Services General Support System (Report No. 4A-CI-00-11-043)

Thank you for providing my office with a copy of the draft report detailing the results of your audit of the Human Resources Solutions (HRS) Center for Talent Services General Support System (CTS GSS). We appreciate the opportunity to comment on the proposed recommendations. Our comments are as follows:

1. **Section VII. Contingency Plan Test**

   OIG Recommendation 1: We recommend HRS conduct a functional contingency plan test for the CTS GSS.

   HRS Response: HRS concurs with the recommendation and will conduct a functional contingency plan test for the CTS GSS during FY12.

   OIG Recommendation 2: We recommend HRS coordinate with the system owners whose systems reside on the CTS GSS to encourage their participation in the functional contingency plan exercises.

   HRS Response: HRS concurs with this recommendation and will coordinate the functional contingency plan test with system owners whose systems reside on the CTS GSS 60 days prior to the actual test.

2. **Section X. NIST SP 800-53 Evaluation, a) PE-13 Fire Protection**

   OIG Recommendation 3: We recommend HRS install a fire suppression system within the Macon facility's computer room.

   HRS Response: HRS employs and maintains a Johnson Controls IFC fire detection and alarm system that is automatically activated in the event of a fire and has been duly inspected and certified. Fire detection devices/systems include hand-held and wheeled fire extinguishers, fixed fire hoses, and state-of-the-art laser smoke detectors. Having an

automatic fire suppression system increases the risk of the suppression agent causing more damage to the equipment than an actual fire. There is minimal material in the room that is combustible thus reducing the potential of a fire spreading. HRTT does not currently employ automatic fire suppression devices due to cost and practicality constraints. HRTT's strategy is to monitor closely and maintain a rapid response capability to enable suppression in a surgical fashion in the event of a fire rather than broadcast a fire suppression agent and affect the entire computer room, making all systems there unreachable for an unacceptable period of time. HRTT has in place a number of countermeasures to reduce the fire risk.

- A Macon fire station is less than two miles away from the facility (Macon-Bibb County Fire Department is A-1 rated).
- The facility is staffed 24/7 by a security guard who is a state-certified, professional law enforcement officer trained as a first responder that has access to the computer room to manually activate the fire suppression mechanisms.
- Existence of a laser smoke detection system in the computer room which employs detectors that are multiple times more sensitive than normal smoke detectors and trigger automatic alarms to the security staff.
- Security guards also perform physical walk-through inspection of all areas every 2 to 4 hours.
- The walls and ceiling of the computer room are made of reinforced concrete and its doors are fire-resistant rated at 1200 degrees Fahrenheit for one hour.

HRS plans to conduct a cost-benefit analysis and formal risk assessment to evaluate the costs and risks of implementing an automatic fire suppression system by the end of FY12 Quarter 2.

3. Section X. NIST SP 800-53 Evaluation, b) PE-1 Physical and Environmental Protection Policy and Procedure

OIG Recommendation 4: We recommend HRS document and implement formal emergency response procedures.

HRS Response: HRS concurs with the recommendation and will document and implement formal emergency response procedures by the end of FY12 Quarter 1.

OIG Recommendation 5: We recommend HRS conduct annual emergency response training.

HRS Response: HRS concurs with this recommendation and will conduct annual emergency response training by the end of FY12 Quarter 2.

If you should need any additional information or have any questions, please contact [redacted]

cc:

[redacted]
Senior Team Leader
Office of Audits
Office of the Inspector General

Janet Barnes
Deputy Director
Internal Oversight and Compliance

[redacted]
Manager
HR Tools and Technology

[redacted]
Designated Security Officer
HR Tools and Technology

[redacted]
Senior Agency Information Security Officer
Office of the Chief Information Officer

Kathleen McGettigan
Deputy Associate Director
Human Resources Solutions

Francis O'H Esquivel
Deputy Associate Director
Leadership and Talent Management Solutions