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

Final Audit Report

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Dashboard Management Reporting System

Report Number 4A-CI-00-14-064
January 14, 2015

-- CAUTION --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Dashboard Management Reporting System

Report No. 4A CI 00 14 064 **January 14, 2015**

Why Did We Conduct the Audit?

The Dashboard Management Reporting System (DMRS) is one of the Office of Personnel Management's (OPM) critical Information Technology (IT) systems. As such, the Federal Information Security Management Act (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.

What Did We Audit?

The OIG has completed a performance audit of DMRS to ensure that the system owner, Federal Investigative Services (FIS), has managed the implementation of IT security policies and procedures in accordance with the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information Security Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

Michael R. Esser
Assistant Inspector General
for Audits

What Did We Find?

Our audit of the IT security controls of DMRS determined that:

- A Security Assessment and Authorization (SA&A) of DMRS was completed in March 2014. We reviewed the authorization package for all required elements of an SA&A, and determined that the package contained all necessary documentation.
- The security categorization of DMRS is consistent with Federal Information Processing Standards (FIPS) 199 and NIST Special Publication (SP) 800-60 requirements, and we agree with the categorization of "High."
- The DMRS System Security Plan contains the critical elements required by NIST SP 800-18 Revision 1.
- A security control assessment plan and report were completed in August 2013 and February 2014, respectively, for DMRS as a part of the system's SA&A.
- FIS ensures security control self-assessments are conducted in accordance with OPM's continuous monitoring methodology.
- A contingency plan was developed for DMRS that is in compliance with NIST SP 800-34 Revision 1, and the plan is tested annually.
- A privacy threshold analysis was conducted for DMRS that indicated that a Privacy Impact Assessment (PIA) was required. A PIA was conducted in November 2013.
- The DMRS Plan of Acton and Milestones (POA&M) follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool. However, the POA&M did not contain information related to estimated remediation costs and resources.
- We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 4 were implemented for DMRS.

  We determined that a majority of tested security controls appear to be in compliance with NIST SP 800-53 Revision 4, however there are potential areas of improvement.

ABBREVIATIONS

DHS	**Department of Homeland Security**
DMRS	**Dashboard Management Reporting System**
FIPS	**Federal Information Processing Standards**
FIS	**Federal Investigative Services**
FISCAM	**Federal Information Security Controls Audit Manual**
FISMA	**Federal Information Security Management Act**
FY	**Fiscal year**
IOC	**Internal Oversight and Compliance**
IT	**Information Technology**
NIST	**National Institute for Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**Office of Management and Budget**
OPM	**Office of Personnel Management**
PIA	**Privacy Impact Assessment**
POA&M	**Plan of Action and Milestones**
PTA	**Privacy Threshold Analysis**
SA&A	**Security Assessment and Authorization**
SAP	**Security Assessment Plan**
SAR	**Security Assessment Report**
SO	**System Owner**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

Page

EXECUTIVE SUMMARY i

ABBREVIATIONS ii

I. **BACKGROUND** 1

II. **OBJECTIVES, SCOPE, AND METHODOLOGY** 2

III. **AUDIT FINDINGS AND RECOMMENDATIONS** 5

1. Security Assessment and Authorization 5
2. FIPS 199 5
3. System Security Plan 6
4. Security Assessment Plan and Report 6
5. Continuous Monitoring 7
6. Contingency Planning and Contingency Plan Testing 7
7. Privacy Impact Assessment 8
8. Plan of Action and Milestones Process 8
9. NIST SP 800-53 Evaluation 9

IV. **MAJOR CONTRIBUTORS TO THIS REPORT** 12

APPENDIX: Federal Investigative Services' October 31, 2014 response to the draft audit report, issued October 14, 2014.

REPORT FRAUD, WASTE, AND MISMANAGEMENT

I. BACKGROUND

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) Dashboard Management Reporting System (DMRS).

DMRS 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.

The DMRS web-based application is designed to support delivery of services to the Federal Investigative Service (FIS), which is responsible for investigative products and services that ensure federal agencies have the data needed on which to base determinations of eligibility for a security clearance or suitability for employment in sensitive positions. The system is operated and hosted by OPM, and owned by FIS.

DMRS is currently operating on [redacted], the system's backend information retrieval application. FIS is in the process of migrating to [redacted], pending approval from OPM's Office of the Chief Information Officer (OCIO). As such, the most recent Security Assessment and Authorization (SA&A) for DMRS was based on [redacted]. While this current SA&A package was reviewed as a part of this audit, the controls referenced throughout this report reflect the controls in place at the time of the audit and are representative of [redacted] which is currently in production for DMRS.

This was our first audit of the security controls surrounding DMRS. We discussed the results of our audit with FIS and OCIO representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objective

Our objective was to perform an evaluation of the security controls for DMRS to ensure that FIS officials have managed the implementation of 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 the OCIO.

OPM's IT security policies require the owners 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 DMRS, including:

- Security Assessment and Authorization;
- Federal Information Processing Standards Publication (FIPS) 199 Analysis;
- System Security Plan;
- Security Assessment Plan and Report;
- 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 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 FIS officials responsible for DMRS, including IT security controls in place as of August 2014.

We considered the DMRS 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 FIS program office with DMRS 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 DMRS 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 DMRS system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM’s 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 3, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Version 2, Volume II: Appendices to 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;
- FIPS 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 OIG, as established by the Inspector General Act of 1978, as amended. The audit was conducted from June through August 2014 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding DMRS.

Compliance with Laws and Regulations

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

1. Security Assessment and Authorization

The SA&A of the DMRS was completed in March 2014. This SA&A package assesses the controls applicable to [redacted] the backend information retrieval application supporting DMRS. FIS is currently in the process of upgrading the system from [redacted]

OPM's Chief Information Security Officer reviewed the DMRS SA&A package and signed the system's authorization letter on March 18, 2014. The system's authorizing official signed the letter and authorized the continued operation of the system on March 19, 2014.

NIST SP 800-37 Revision 1, Guide for Applying Management Framework to Federal Information Systems, provides guidance to federal agencies in meeting security accreditation requirements. The DMRS SA&A appears to have been conducted in compliance with NIST requirements.

2. FIPS 199

FIPS 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 Version 2, Volume II: Appendices to 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 DMRS FIPS 199 Security Categorization documentation contains an analysis of information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. DMRS is categorized with a high impact level for confidentiality, moderate for integrity, moderate for availability, and an overall categorization of "High."

The security categorization of DMRS is consistent with FIPS 199 and NIST SP 800-60 requirements, and we do not disagree with the categorization of "High."

3. System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 3[1], 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 a System Security Plan (SSP) for each system, and provides guidance for doing so.

The SSP for DMRS was created using the template outlined in NIST SP 800-18 Revision 1. The template requires that the following elements be documented within the SSP:

- 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.

We reviewed the DMRS SSP and determined that it adequately addresses each of the elements required by NIST. Nothing came to our attention to indicate that the system security plan of DMRS has not been properly documented and approved.

4. Security Assessment Plan and Report

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for DMRS in August 2013 and February 2014, respectively, as a part of the system's SA&A process. The SAP and SAR were completed by a contractor that was operating independently from FIS. We reviewed the documents to verify that a risk assessment was conducted in

[1] Revision 4 to NIST SP 800-53 was released in April 2013. OPM allows systems one year to implement the controls for the new revision. The SA&A package was completed in March 2014 for this audit; therefore we used Revision 3 as criteria to review the DRMS SSP.

accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a "High" security categorization according to NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems.

The SAP outlined the assessment approach, scanning authorization, and test methodology. The SAR identified several control weaknesses, and these weaknesses were appropriately added to the DMRS POA&M for tracking.

Nothing came to our attention to indicate that the security controls of DMRS have not been adequately tested by an independent source.

5. Continuous Monitoring

OPM's Information Security and Privacy Policy Handbook states that continuous monitoring security reports must be provided to the OCIO's Information Technology Security and Privacy Group (ITSP) at least semiannually. The OCIO also creates continuous monitoring plans each fiscal year that clearly describe the type and frequency of NIST SP 800-53 Revision 4 security controls that must be tested throughout the year.

In FY 2013, FIS submitted adequate evidence of continuous monitoring security control testing for DMRS to ITSP in a timely manner. The SA&A of the DMRS was completed in March 2014; the SAR included in the SA&A package meets the OPM continuous monitoring reporting requirement for 2014.

Nothing came to our attention to indicate FIS' continuous monitoring activities were not in compliance with OPM guidelines.

6. 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 DMRS contingency plan documents the functions, operations, and resources necessary to restore and resume DMRS operations when unexpected events or disasters occur. The DMRS contingency plan adequately follows the format suggested by NIST SP 800-34 Revision 1 and contains the required elements.

Contingency Plan Test

NIST SP 800-34 Revision 1 provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability. A failover and failback test of the DMRS was conducted in February 2014. The test involved failing over to the backup data center and then returning operations to the regular data center. The testing documentation contained an analysis and review of the results.

7. Privacy Impact Assessment

The E-Government Act of 2002 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.

FIS completed an initial privacy screening or Privacy Threshold Analysis of DMRS and determined that a PIA was required for this system. A PIA was conducted in November 2013 and approved by the system owner and CIO.

8. Plan of Action and Milestones Process

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.

We evaluated the DMRS POA&M and verified that it follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool, for evaluation. We determined that the weaknesses discovered during the SA&A security assessment were included in the POA&M. We also reviewed prior POA&M items for proper documentation and closure.

OPM's POA&M Standard Operating Procedures require program offices to analyze and estimate the funding resources required to resolve identified security weaknesses. However, each security weakness identified on the DMRS POA&M references the exact same estimated resources and costs. Due to the varying complexity of the weaknesses contained in this POA&M, we would expect significant variances for the estimated resources required to address each item. Therefore, it is our opinion that these POA&M items were not adequately analyzed on an individual basis.

Failure to correctly estimate remediation costs and resources increases the risk these items are not resolved appropriately and timely.

Recommendation 1

We recommend that FIS review and update the DMRS POA&M with remediation costs and resources that accurately reflect what is necessary to resolve each individual weakness.

FIS Response:

“FIS agrees with the OIG recommendation. A review of the DMRS POA&M will be conducted to determine if the remediation costs and resources are accurately identified and revise as needed.”

OIG Reply:

As part of the audit resolution process, we recommend that FIS provide OPM’s Internal Oversight and Compliance (IOC) division with evidence that it has adequately implemented this recommendation. This statement also applies to all subsequent recommendations in this audit report that FIS agrees to implement.

9. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 4[2], 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 implemented for DMRS. We tested approximately 55 security controls outlined in NIST SP 800-53 Revision 4 that were identified as being system specific or a hybrid control. Controls identified as common or inherited were omitted from testing because another system or program office is responsible for implementing the control. We tested one or more controls from each of the following control families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Media Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communication Protection

[2] Revision 4 of NIST SP 800-53 was released in April 2013. OPM allows systems one year to implement the controls for the new revision. The control testing performed for this audit took place in August 2014; therefore, we used Revision 4 as criteria for our testing of DMRS security controls.

- Identification and Authorization
- System and Information Integrity

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

We determined that the tested security controls appear to be in compliance with NIST SP 800-53 Revision 4 requirements, with the following exceptions:

1. Control Family AU - Audit and Accountability

The [redacted] utilized by DMRS does not support any auditing capabilities. This lack of functionality has prompted the migration to [redacted], which has the technical capability to audit and track events in the system.

NIST SP 800-53 Revision 4 requires that "The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event."

Failure to log and audit system events increases the risk that unauthorized events are occurring on the system.

Recommendation 2

We recommend that FIS implement technical controls on DMRS to track system events in accordance with the NIST SP 800-53 Revision 4 Audit and Accountability control family.

FIS Response:

"FIS agrees with the OIG recommendation. FIS, in collaboration with the OCIO is currently developing specific design requirements to satisfy the Audit and Accountability control families in the [redacted] environment."

Recommendation 3

We recommend that FIS review its auditing and accountability policies and procedures and incorporate the technical controls implemented as part of Recommendation 2.

FIS Response:

"FIS agrees with the OIG recommendation. A review of the auditing and accountability policies and procedures will be conducted in concert with the implementation of auditing and accountability features implemented as part of Recommendation 2."

2. **Control CA-8 -** [redacted]

FIS does not currently conduct [redacted] for DMRS.

NIST SP 800-53 Revision 4 requires [redacted] to be performed for systems with a security categorization of high. Accordingly, OPM's Information Security and Privacy Policy Handbook states that "OPM shall include as part of security assessments, [redacted]"

Failure to [redacted] increases the risk of unauthorized activity and data loss.

<u>Recommendation 4</u>

We recommend that FIS implement policies and procedures to conduct routine [redacted] on DMRS.

<u>FIS Response:</u>

"FIS respectfully disagrees with the OIG recommendation. Current OPM Information Security and Privacy Policy, does not require [redacted] In consultation with the OPM-OCIO-ITSP, it is our understanding that the proposed update to the policy in accordance with NIST 800-53 Rev. 4 will recommend [redacted] for [systems that are outward facing]. Please note that the OPM-FIS Dashboard Management Reporting System (DMRS) is not an outward facing system. As such, we request reconsideration of OIG Recommendation 4."

<u>OIG Reply:</u>

OPM's current version of the Information Privacy and Policy Handbook and NIST SP 800-53 Revision 4 requires system's with a high security categorization to conduct [redacted] As such, we continue to recommend that FIS implement policies and procedures to conduct [redacted] on DMRS. As part of the audit resolution process, we recommend that FIS provide OPM's IOC division with evidence that it has adequately addressed this audit finding.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted] Auditor-In-Charge

[redacted] IT Auditor

[redacted] IT Auditor

[redacted] Group Chief

Appendix

United States Office of Personnel Management

TO: [redacted]
Chief, Information Systems Audits Group

FROM: [redacted]
Dashboard Management Reporting System (DMRS) System Owner
Chief, IT System Security & Access
Federal Investigative Services

SUBJECT: Response to Draft Report No. 4A-IS-00-14-064 – Dated - October 14, 2014

OIG Recommendation 1: We recommend FIS review and update the DMRS POA&M with remediation costs and resources that accurately reflect what is necessary to resolve each individual weakness.

FIS Response: FIS agrees with the OIG recommendation. A review of the DMRS POA&M will be conducted to determine if the remediation costs and resources are accurately identified and revise as needed.

OIG Recommendation 2: We recommend that FIS implement technical controls on DMRS to track system events in accordance with the NIST SP 800-53 Audit and Accountability control family.

FIS Response: FIS agrees with the OIG recommendation. FIS, in collaboration with the OCIO is currently developing specific design requirements to satisfy the Audit and Accountability control families in the [redacted] environment.

OIG Recommendation 3: We recommend FIS review its auditing and accountability policies and procedures and incorporate technical controls implemented as part of Recommendation 2.

FIS Response: FIS agrees with the OIG recommendation. A review of the auditing and accountability policies and procedures will be conducted in concert with the implementation of auditing and accountability features implemented as part of Recommendation 2.

OIG Recommendation 4: We recommend that FIS implement policy and procedures to conduct [redacted] on DMRS.

FIS Response: FIS respectfully disagrees with the OIG recommendation. Current OPM Information Security and Privacy Policy, does not require [redacted] In consultation with the OPM-OCIO-ITSP, it is our understanding that the proposed update to the policy in accordance with NIST 800-53 Rev. 4 will recommend [redacted] for *[systems that are outward facing*]”. Please note that the OPM-FIS Dashboard Management Reporting System (DMRS) is not an outward facing system. As such, we request reconsideration of OIG Recommendation 4.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100

-- CAUTION --

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage (*http://www.opm.gov/our-inspector-general*), caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.