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 AUDIT REPORT & RECEIVABLES TRACKING SYSTEM FY 2012

Report No. 4A-OP-00-12-013

Date: July 16, 2012

--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 prntected by Fcderal law (18 U.S.C. 1905). Therefore, whilc this audit repnrt is available under the Freedom of Information Act and made available to thc public on the OIG webpage, caution needs to bc cxercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

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 AUDIT REPORT & RECEIVABLES TRACKING SYSTEM FY 2012

WASHINGTON, D.C.

Report No. 4A-OP-00-12-013

Date: 07/16/12

Michael R. Esser
Assistant Inspector General
for Audits

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administratioa 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, 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.

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 AUDIT REPORT & RECEIVABLES TRACKING SYSTEM FY 2012

WASHINGTON, D.C.

Report No. 4A-OP-00-12-013

Date: 07/16/12

This final audit report discusses the results of our review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Audit Report & Receivables Tracking System (ARRTS). Our conclusions are detailed in the "Results" section of this report.

The Office of the Inspector General (OIG) reviewed the ARRTS security program and found that ARRTS is inappropriately classified as a major application on the agency's system inventory. We have recommended that ARRTS be reclassified as a minor application under OPM's Local Area Network/Wide Area Network general support system.

Through the course of our review we determined that the following areas appeared to be in full FISMA compliance:

- A security certification and accreditation (C&A) of ARRTS was completed in February 2010.
- The OIG agrees with the security categorization of "low" for ARRTS.
- The Information System Security Plan for ARRTS contains the critical elements required by National Institute of Standards and Technology Special Publication (NIST SP) 800-18.

- A risk assessment was conducted for ARRTS as a part of its 2010 C&A that addresses all the required elements outlined in relevant NIST guidance.
- A Privacy Threshold Analysis was conducted for ARRTS determining that a Privacy Impact Assessment was not required for this system.

However, we noted the following opportunities for improvement in the ARRTS security program:

- An independent security test and evaluation was completed for ARRTS as a part of the system's C&A process; however, all security controls were not adequately tested.
- The designated security officer for ARRTS did not conduct a self-assessment of the system.
- A contingency plan for ARRTS does not contain all elements required by NIST SP 800-34 and has not been tested.
- The ARRTS Plan of Action and Milestones contains security weaknesses that are significantly overdue.
- The OIG independently tested 37 of the NIST SP 800-53 controls for ARRTS and found that many of these security controls were not in place during the fieldwork phase of the audit. We found that the following security controls were not fully implemented for ARRTS:
    - AT-3 Security Training
    - AU-2 Auditable Events
    - AU-3 Content of Audit Records
    - AU-6 Audit Review, Analysis, & Reporting
    - AU-9 Protection of Audit Information
    - AU-11 Audit Record Retention
    - AU-12 Audit Generation
    - IA-4 Identifier Management
    - PS-4 Personnel Termination
    - PS-5 Personnel Transfer
    - PS-6 Access Agreements
    - RA-5 Vulnerability Scanning
    - CM-6 Configuration Settings

Contents

Page

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) Audit Report & Receivables Tracking System (ARRTS).

Background

Ownership of ARRTS is shared between OPM's Office of the Inspector General (OIG), Office of the Chief Financial Officer (OCFO), and the Healthcare and Insurance Office (HIO). While these three offices, (referred to as "the Owners") collectively own and use the system, ARRTS resides on OPM's Local Area Network / Wide Area Network (LAN/WAN) general support system and is supported by individuals within the Office of the Chief Information Officer's (OCIO) Benefit Systems Group. The purpose of the ARRTS application is to track audits, audit recommendations, and receivables resulting from audits of OPM programs and contracts pertaining to the Federal Employees Health Benefits Program and the Federal Employees' Group Life Insurance Program. ARRTS is comprised of three main modules: 1) the Audit Management Module (used by all three Owners of ARRTS), 2) the Financial Management Module (used by OCFO and HIO), and 3) the System Administration Module used only by the system administrator and designated security professionals.

Objectives

Our objective was to perform an evaluation of the security controls for ARRTS to ensure that the Owners of ARRTS 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 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 ARRTS, 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 (NIST 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 the Owners of ARRTS, including IT security controls in place as of January 2012.

We considered the ARRTS 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 OIG, OCFO, HIO, and OCIO divisions and other individuals with security responsibilities for ARRTS. 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 ARRTS 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 ARRTS 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, 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 (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 Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from November 2011 through January 2012 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding ARRTS.

Compliance with Laws and Regulations

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

Results

I. Certification and Accreditation Statement

A security certification and accreditation (C&A) of ARRTS was completed in February 2010.

OPM's Acting IT Security Officer (representing the OCIO) reviewed the ARRTS C&A package and signed the system's certification package on February 18, 2010. The system's designated accrediting authority, the Deputy Inspector General, signed the accreditation statement and authorized the continued operation of the system on February 19, 2010.

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. Several elements of the ARRTS C&A package were not completed in full compliance with NIST requirements, including: Independent Security Control Testing, Security Control Self Assessment, Contingency Plan & Contingency Plan Testing, and Plan of Action and Milestones Process. The specific problems we identified in each of these areas are detailed in the sections below.

In addition, the certification and accreditation occurred several months past the 3 year timeline required by NIST.

OPM's OCIO created and published guidance for preparing and conducting C&As in January 2011. These policies and procedures are now in effect for all OPM systems. However, the ARRTS C&A was appropriately conducted in accordance with the guidance available in 2010.

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 ARRTS FIPS 199 categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. ARRTS is categorized with a low impact level for confidentiality, integrity, and availability, resulting in an overall categorization of low. The security categorization of ARRTS appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and the OIG agrees with the categorization of low.

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 Information System Security Plan (ISSP) for each system, and provides guidance for doing so.

The ISSP for ARRTS was created using a template that is outlined in NIST SP 800-18. The ISSP contains the key elements outlined in the NIST guide.

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 ARRTS as a part of the 2010 C&A. All major elements outlined in the NIST guidance were addressed.

V. Independent Security Control Testing

A security assessment was completed for ARRTS in December 2009 as a part of the system's C&A process. The security assessment was conducted by another government agency, the Bureau of Public Debt (BPD). 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 "low" security categorization according to NIST SP 800-53, Recommended Security Controls for Federal Information Systems. Our review determined that the security controls of ARRTS have not been adequately tested.

The BPD only examined 28 of the over 100 controls applicable to a FIPS 199 "low" categorized system. Eighty-eight controls were listed as not applicable to ARRTS. Of those 88, 82 were listed as common controls inherited from either OPM or the LAN/WAN, 1 was listed as a hybrid control and 5 were outright omitted from testing. However, OPM's common controls catalog only identifies 24 controls that can be inherited by other systems, and therefore it is not possible for ARRTS to inherit 82 controls. Furthermore, our testing during this audit revealed that at least 11 of the security controls BPD listed as "not applicable" were not fully implemented for ARRTS (see section X, below, for details).

FISMA requires that all NIST SP 800-53 controls applicable to the system be tested every three years by an independent source. Inappropriately omitting controls from security control testing increases the risk that security weaknesses remain undetected.

Recommendation 1

We recommend that an independent test of the system's security controls be conducted for ARRTS that fully tests all controls applicable to a FIPS 199 "low" system as mandated by NIST SP 800-53.

System Owners' Response:

"We concur with the recommendation and ARRTS is expected to transition to the OPM OCIO to be placed under the LAN/WAN GSS. Preparations are being made between the OCIO and the Office of the Inspector General (OIG) to conduct a thorough test of security controls."

OIG Reply:

As part of the audit resolution process, for all recommendations where the System Owners are in agreement with our recommendation, we recommend that the System Owners provide Internal Oversight and Compliance (IOC) with evidence supporting the remediation of the recommendation.

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 security assessment is not being conducted on a system, the system's owner must conduct an internal self-assessment of security controls. Furthermore, NIST SP 800-53 mandates the development of a security assessment plan and outlines the required inclusions.

The DSO of ARRTS did not conduct a self-assessment of the system in 2011.

Failure to complete a security controls test increases the risk that IT security weaknesses are undetected and that the Owners of ARRTS are unable to make informed judgments to appropriately mitigate risks to an acceptable level.

Recommendation 2

We recommend that the Owners of ARRTS ensure that the annual test of security controls is completed for ARRTS.

System Owners' Response:

"We concur with the recommendation. Preparations are being made to conduct an internal self-assessment of security controls and plans will be put in place to ensure this occurs on an annual basis."

VII. Contingency Planning and Contingency Plan Testing

NIST SP 800-34, Contingency Planning Guide for IT 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.

<u>Contingency Plan</u>

The ARRTS contingency plan documents the functions, operations, and resources necessary to restore and resume ARRTS operations when unexpected events or disasters occur. The ARRTS contingency plan generally follows the format suggested by NIST SP 800-34 and contains a majority of the suggested elements.

However, there are several areas for improvement within the contingency plan. The contingency plan had inconsistencies with regard to back-up procedures, did not have complete contact information for critical individuals, and contained a significantly outdated Memorandum of Understanding. Furthermore, the Owners of ARRTS did not review the contingency plan in 2011.

Failure to maintain a thorough contingency plan decreases the likelihood that the system can remain operable should unexpected events or disasters occur.

<u>Recommendation 3</u>

We recommend that the Owners of ARRTS revise the system’s contingency plan to ensure it encompasses all requirements outlined in NIST SP 800-34.

<u>System Owners’ Response:</u>

“We concur with the recommendation and the ARRTS Contingency Plan is being rewritten into the updated template provided by the OCIO. The primary Contingency Plan will be the plan for the LAN/WAN GSS and the Contingency Plan for ARRTS will address contacts and actions that will be needed specifically for ARRTS in the event of a situation.”

<u>Recommendation 4</u>

We recommend that the Owners of ARRTS implement a process for annually reviewing the contingency plan.

<u>System Owners’ Response:</u>

“We concur with the recommendation and will implement a plan to annually review the ARRTS contingency plan. A plan is currently underway to conduct a table top exercise designed to review and test the Contingency Plan.”

<u>Contingency Plan Test</u>

NIST SP 800-34, Contingency Planning Guide for Information Technology, provides guidance for testing contingency plans and documenting the results. In addition, NIST SP 800-53 Control CP-3 requires system owners to train “personnel in their contingency roles and responsibilities to the information system and provide refresher training.”

The Owners of ARRTS did not conduct a test of the system’s contingency plan in 2011.

Contingency plan testing is a critical element of a viable disaster recovery capability. Failure to routinely test the contingency plan decreases the likelihood that the system can remain operable should unexpected events or disasters occur.

Recommendation 5

We recommend that the Owners of ARRTS test the system’s contingency plan on an annual basis.

System Owners’ Response:

“We concur with the recommendation and the OCIO and the three ARRTS stakeholders will conduct an annual test of the ARRTS Contingency Plan.”

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 PTA. If the PTA reveals that the system collects no information in identifiable form, for example, the Privacy Program Manager will indicate in the PTA review that no PIA is required. The PTA must be incorporated into the system’s certification and accreditation (C&A) package.”

The Owners of ARRTS completed a Privacy Threshold Analysis (PTA) of ARRTS and determined that a PIA was not required for this system because it does not contain Personally Identifiable Information (PII). The OIG agrees with this conclusion.

IX. Plan of Action and Milestones Process

A Plan of Action and Milestones (POA&M) is a tool, mandated by NIST SP 800-53 Control CA-5, 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 ARRTS 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 entries for all security weaknesses identified through various security control tests and audits. However, the Owners of ARRTS are not utilizing the POA&M process effectively. The ARRTS POA&M contained 10 security weaknesses, the majority of which have remediation activities in excess of 400 days overdue. In addition, the ARRTS POA&M does not contain the specific recommended corrective action, or provide detail to specific milestones or action items required to address the weakness. Each POA&M item typical only states that a solution will be discussed, documented, and implemented.

Failure to use the POA&M processes to address known security weaknesses in a timely manner increases the risk that someone could gain unauthorized access to the system or the data it contains.

Recommendation 6

We recommend that the Owners of ARRTS revise the POA&M items currently listed to include the recommended corrections, milestones, and action items, rather than just identifying the weaknesses.

System Owners' Response:

"We concur with the recommendation and will implement the changes to the current POA&M items. As soon as ARRTS is transitioned to the OCIO, the ARRTS stakeholders will coordinate with the OCIO for remediation of the existing POA&Ms, tracking their progress, and adding new vulnerabilities as they are identified."

Recommendation 7

We recommend that the Owners of ARRTS develop a plan for the immediate remediation of all overdue POA&M items.

System Owners' Response:

"We concur with the recommendation and will review the current POA&M items. As ARRTS is transitioned to the OCIO, the stakeholders will coordinate with the OCIO for the remediation of the existing POA&Ms."

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 whether a subset of these controls had been implemented for ARRTS. We tested 37 of the approximately 100 security controls outlined in NIST SP 800-53 Revision 3 that are applicable to a FIPS 199 "low" categorized system. We tested the following controls:

- Access Control: AC-14, AC-17, AC-18, AC-19, AC-20, & AC-22
- Awareness and Training: AT-3
- Audit and Accountability: AU-2, AU-3, AU-6, AU-9, AU-11, & AU-12
- Security Assessment and Authorization: CA-2, CA-3, CA-5, & CA-6
- Configuration Management: CM-2, CM-6, & CM-7
- Contingency Planning: CP-2, CP-3, CP-9, & CP-10
- Identification and Authentication: IA-4 & IA-8
- Maintenance MA-4 & MA-5
- Personnel Security: PS-2, PS-4, PS-5, PS-6, & PS-7
- Risk Assessment: RA-5
- System and Services Acquisition: SA-9
- System and Communication Protection: SC-14 & SC-15

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

Through our testing we determined that many of the NIST SP 800-53 security controls applicable to ARRTS have not been successfully implemented.

a) AT-3 Security Training

Not all individuals with significant IT responsibility for ARRTS have been identified by the Owners of the system. As a result, OPM's IT Security and Privacy Group (ITSPG) is unable to track training completed by individuals with IT responsibility, as required by FISMA.

NIST SP 800-53 control AT-3 mandates that "The organization provides role-based security-related training: (1) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [annually, as designated by OPM policy] thereafter."

Failure to properly document and report security training to the ITSPG increases the likelihood that individuals with significant IT responsibilities for ARRTS do not receive the appropriate annual training for their position.

Recommendation 8

We recommend that the Owners of ARRTS identify the individuals with significant IT responsibility for ARRTS that require specialized IT security training.

System Owners' Response:

"We concur with the recommendation and a list of individuals from the OIG that have significant IT responsibility for ARRTS will be compiled and those names will be supplied to the OCIO to ensure that these individuals receive specialized IT security training annually."

Recommendation 9

We recommend that the Owners of ARRTS ensure that all employees with significant information security responsibility for ARRTS take meaningful and appropriate specialized security training on an annual basis.

System Owners' Response:

"We concur with the recommendation and the OIG will add a POA&M to the OIG LAN POA&Ms that requires the tracking of the annual security training for all staff that has significant IT responsibilities. A report pertaining to the staff training will be provided to the OCIO."

b) AU-2 Auditable Events, AU-3 Content of Audit Records, AU-6 Audit Review, Analysis & Reporting, AU-9 Protection of Audit Information, AU-11 Audit Record Retention, & AU-12 Audit Generation

The management of audit logs for ARRTS could be improved.

Database level auditing is not currently enabled for ARRTS. Oracle10 has the capability to perform audit functions. However, a list of auditable events has not been developed by the system's Owners. ARRTS uses a single Oracle account to access the database, and therefore the database logs cannot distinguish the transactions conducted by various User IDs. This fact should be taken into consideration when determining the events to log, but should not be justification against auditing database changes. Furthermore, auditing should still be implemented at the application level. Transaction level detail should be logged, protected from alteration, and routinely reviewed by the Owners of ARRTS.

Failure to routinely log and review user activity increases the risk that fraudulent or malicious activity can occur undetected.

Recommendation 10

We recommend that the Owners of ARRTS develop an audit policy that contains a list of events that should be logged for ARRTS at the database and application levels.

System Owners' Response:

"We concur with the recommendation and the OCIO and the three stakeholders will develop an audit policy that contains a list of events that should be logged."

Recommendation 11

We recommend that the ARRTS system be modified to generate audit logs in accordance with audit policy and in compliance with all applicable NIST SP 800-53 standards.

System Owners' Response:

"We concur with the recommendation and ARRTS will be evaluated for the feasibility of implementing system modifications to generate audit logs that are in compliance with NIST SP 800-53 standards."

Recommendation 12

We recommend that ARRTS be modified to ensure all audit logs cannot be inappropriately accessed, modified, or deleted.

System Owners' Response:

"We concur with the recommendation and ARRTS will be evaluated for the feasibility of system modifications to ensure that audit logs cannot be inappropriately accessed, modified, or deleted."

Recommendation 13

We recommend that the Owners of ARRTS routinely monitor/review audit logs generated by ARRTS.

System Owners' Response:

"We concur with the recommendation and procedures will be put in place to ensure that ARRTS audit logs are routinely monitored and reviewed."

c) IA-4 Identifier Management

There are individuals that have multiple user accounts for ARRTS.

NIST SP 800-53 requires that System Owners manage "information system identifiers for users by: … Selecting an identifier that uniquely identifies an individual… [and] preventing reuse of user . . . identifiers . . . ."

Assigning multiple accounts to one user increases the risk that individuals can gain unauthorized access to ARRTS data.

Recommendation 14

We recommend that the Owners of ARRTS disable/delete unnecessary duplicate ARRTS user accounts.

System Owners' Response:

"We concur with the recommendation however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. Access to the ARRTS system requires that a user first log into the OPM LAN with a valid user ID and password. If an OPM staff member is terminated, retires, or leaves the agency they no longer have access to the OPM LAN and as a result they can no longer access the ARRTS application. If the employee changes jobs within OPM and no longer requires access to ARRTS, documented procedures will be in place to ensure that the ARRTS application is removed from that individual's computer. While there may be a low level risk still associated with outdated user IDs remaining active in ARRTS, we believe the level of risk is extremely low. This matter will require a Business Case Exception to be developed and approved to accept this risk."

OIG Reply:

OPM's Information Security and Privacy Policy Handbook states that "The information system shall uniquely identify and authenticate organizational users" and requires that "Information system identifiers for users and devices . . . be managed by: . . . Preventing reuse of user or device identifiers permanently."

Proper maintenance of user accounts is an important security control, and accepting the risk of maintaining duplicate user accounts is not appropriate in this case. We recommend that a system modification be made to facilitate the prompt removal of duplicate users' system level access to ARRTS.

<u>Recommendation 15</u>

We recommend that the Owners of ARRTS implement a process to routinely audit all active user accounts to ensure that no unnecessary duplicate accounts exist.

<u>System Owners' Response:</u>

"We concur with the recommendation and will implement a process to routinely review all active user accounts in ARRTS however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. . . ."

<u>OIG Reply:</u>

As stated above, it is not appropriate to accept the risks associated with the inability to appropriately manage user accounts. We recommend that a system modification be made to facilitate the prompt removal of duplicate users' system level access to ARRTS and that an audit process be implemented to ensure duplicate accounts do not exist.

d) PS-4 Personnel Termination

User IDs are never removed or disabled from ARRTS, and IDs for a significant number of individuals remain active after the individuals' employment was terminated. Disabling ARRTS application accounts after a user is terminated provides an extra layer of control to ensure that unauthorized users cannot access the system.

NIST SP 800-53 requires System Owners to ensure that "upon termination of individual employment: . . .Terminate information system access."

<u>Recommendation 16</u>

We recommend that the Owners of ARRTS disable active user accounts that belong to terminated employees.

<u>System Owners' Response:</u>

"We concur with the recommendation however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. . . ."

<u>OIG Reply:</u>

Access to ARRTS is not restricted by terminal or synced with the user's LAN account, thus removing the ARRTS application from the individual's computer and disabling a LAN account does not prevent an individual from using that user ID and password to gain access to ARRTS from any other terminal where the application is loaded. Therefore, accepting the risk of maintaining user accounts after termination is not an appropriate course of action. We recommend that a system modification be made to facilitate the prompt removal of terminated users' system level access to ARRTS.

Recommendation 17

We recommend that the Owners of ARRTS periodically audit active ARRTS user accounts to verify that accounts do not remain open for individuals no longer employed at OPM and that the level of access granted remains appropriate.

System Owners' Response:

"We concur with the recommendation and will implement procedures requiring periodic audits of active ARRTS user accounts however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. . . ."

OIG Reply:

As mentioned above, it is not appropriate to accept the risk associated with ARRTS inability to disable or remove user accounts. We continue to recommend that a system modification be made to ARRTS that enables the system owners to promptly disable active user accounts that belong to terminated employees.

e) PS-5 Personnel Transfer

There are a substantial number of individuals with active user IDs that do not currently have a business reason to have access to ARRTS.

NIST SP 800-53 requires the System Owners to review "logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization . . . ."

Maintaining active user IDs for individuals who do not have a business reason to have access to ARRTS increases the risk that individuals can inappropriately access ARRTS data.

Recommendation 18

We recommend that the Owners of ARRTS disable/delete unnecessary user IDs for users who no longer have a business reason to have access to ARRTS.

System Owners' Response:

"We concur with the recommendation however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. . . ."

<u>OIG Reply:</u>

As mentioned above, it is not appropriate to accept the risk associated with ARRTS inability to disable or remove user accounts. We continue to recommend that a system modification be made to ARRTS that enables the system owners to promptly disable active user accounts that belong to terminated employees.

f) PS-6 Access Agreements

ARRTS users are not required to sign a rules of behavior document.

NIST SP 800-53 requires the System Owners to ensure "that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access."

Failure to require users to sign access agreements increases the likelihood that users will inappropriately access or manipulate information within ARRTS.

<u>Recommendation 19</u>

We recommend that the Owners of ARRTS develop a Rules of Behavior/Acceptable Use Statement for ARRTS and ensure it is signed by all users.

<u>System Owners' Response:</u>

"We concur with the recommendation and the OIG will implement a Rules of Behavior/Acceptable Use document specifically for ARRTS to be signed by all current and future ARRTS users."

g) RA-5 Vulnerability Scanning

Vulnerability scanning is not conducted for ARRTS.

NIST SP 800-53 mandates that vulnerability scanning is conducted, vulnerability scan reports be analyzed, and that legitimate vulnerabilities be remediated.

Not conducting vulnerability scans increases the likelihood that vulnerabilities within the system go undetected and that system weaknesses could be exploited.

<u>Recommendation 20</u>

We recommend that the Owners of ARRTS ensure that routine vulnerability scans are conducted on the system.

<u>System Owners' Response:</u>

"We concur with the recommendation and as soon as ARRTS is transitioned to the OCIO's LAN/WAN GSS, the OCIO plans to do routine vulnerability scans."

h) CM-6 Configuration Settings

The OIG conducted vulnerability scans of the database and server supporting ARRTS using AppDetective Pro and Nessus scanning tools. Although the technical details of these settings will not be included in this report, the Owners of ARRTS and the administrators responsible for this database and server have been provided with this information.

The vulnerability scans revealed that both the database and server contain settings configured in a manner not fully compliant with OPM's configuration policies.

NIST SP 800-53 requires that the Owners of ARRTS ensure that the system is configured such that it "reflects the most restrictive mode consistent with operational requirements" and contains "configuration settings in accordance with organizational policies and procedures."

Maintaining configurations outside of OPM policies greatly increases the likelihood that the configuration weaknesses could be exploited to gain unauthorized access to the system.

Recommendation 21

We recommend that the database supporting ARRTS be configured in a manner that is compliant with OPM's policies.

System Owners' Response:

"We concur with the recommendation and will coordinate with the OCIO to ensure that the database and server is configured in a manner that is compliant with OPM's policies."

Recommendation 22

We recommend that the server supporting ARRTS be configured in a manner that is compliant with OPM's policies.

System Owners' Response:

"We concur with the recommendation [and] will coordinate with the OCIO to ensure that ARRTS is compliant with OPM policies."

XI. Classification of ARRTS as a Minor Application

ARRTS is currently classified as a "major application" and is included on OPM's master inventory of major systems. However, as mentioned in section II, above, ARRTS is designated with a FIPS 199 "low" security categorization. NIST SP 800-18 states that "A major application is expected to have a FIPS 199 impact level of moderate or high." Therefore, an application with a "low" categorization such as ARRTS should not be included as a major application on the agency's system inventory.

OPM's LAN/WAN general support system (owned and operated by the OCIO) currently supports a variety of minor applications. Considering the OCIO currently provides technical support for ARRTS and the system already resides within the boundaries of the LAN/WAN, we believe that ARRTS should be reclassified as a minor application within the LAN/WAN.

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

Although transitioning ARRTS to a minor application would alleviate some of the C&A related requirements that major systems are subject to, it does not absolve the Owners of the system from ensuring the remediation of the extensive security weaknesses identified in prior security assessments and this audit report.

Recommendation 23

We recommend that the Owners of ARRTS work with the OCIO to reclassify ARRTS as a minor application within the LAN/WAN general support system.

System Owners' Response:

"We concur with the recommendation and a Memorandum of Understanding is being developed in anticipation of the downgrade of ARRTS to a minor application system and the transition of ARRTS to the OPM LAN/WAN GSS."

Recommendation 24

We recommend that the OCIO update the LAN/WAN ISSP to reflect ARRTS as a minor application.

System Owners' Response:

"We concur with the recommendation and we are currently working with the OCIO to downgrade ARRTS to a minor application. We will work closely with the OCIO to ensure that the LAN/WAN ISSP is updated to reflect ARRTS as a minor application."

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

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

March 21, 2012

MEMORANDUM FOR [redacted]
Chief, Information Systems Audit Group

FROM: NORBERT E. VINT
Deputy Inspector General Norbert E. Vint

SUBJECT: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Audit Report & Receivables Tracking System (Report No. 4A-OP-00-12-013)

Thank you for providing us with a copy of the draft audit report detailing the results of our fiscal year 2012 audit of the U.S. Office of Personnel Management's (OPM) Audit Report & Receivables Tracking System (ARRTS) compliance with the Federal Information Security Management Act (FISMA), as well as OPM's information technology policies and procedures.

The Office of the Inspector General has been coordinating with the Office of the Chief Information Officer (OCIO) to downgrade ARRTS to a minor application system supported by the OPM Local Area Network/Wide Area Network General Support System (LAN/WAN GSS). Our audit responses reflect the likelihood that the ARRTS downgrade will occur in the very near future and that a Memorandum of Understanding will be in place to govern the relationship between the ARRTS stakeholders and the OCIO.

Our comments in response to the audit recommendations are contained below. These responses have been coordinated with the ARRTS stakeholders.

Independent Security Control Testing

Recommendation 1
We recommend that an independent test of the system's security controls be conducted for ARRTS that fully tests all controls applicable to a FIPS 199 "low" system as mandated by NIST 800-53.

Response 1
We concur with the recommendation and ARRTS is expected to transition to the OPM OCIO to be placed under the LAN/WAN GSS. Preparations are being made between the OCIO and the Office of the Inspector General (OIG) to conduct a thorough test of security controls.

Security Control Self-Assessment

Recommendation 2

We recommend that the Owners of ARRTS ensure that the annual test of security controls is completed for ARRTS.

Response 2

We concur with the recommendation. Preparations are being made to conduct an internal self-assessment of security controls and plans will be put in place to ensure this occurs on an annual basis.

Contingency Plan

Recommendation 3

We recommend that the Owners of ARRTS revise the Contingency Plan to ensure it encompasses all requirements outlined in NIST 800-53 CP-2 Contingency Plan.

Response 3

We concur with the recommendation and the ARRTS Contingency Plan is being rewritten into the updated template provided by the OCIO. The primary Contingency Plan will be the plan for the LAN/WAN GSS and the Contingency Plan for ARRTS will address contacts and actions that will be needed specifically for ARRTS in the event of a situation.

Contingency Plan Testing

Recommendation 4

We recommend that the Owners of ARRTS implement a process for annually reviewing the Contingency Plan.

Response 4

We concur with the recommendation and will implement a plan to annually review the ARRTS contingency plan. A plan is currently underway to conduct a table top exercise designed to review and test the Contingency Plan.

Recommendation 5

We recommend that the Owners of ARRTS test the system's contingency plan on an annual basis.

Response 5

We concur with the recommendation and the OCIO and the three ARRTS stakeholders will conduct an annual test of the ARRTS Contingency Plan.

Plan of Action and Milestones (POA&Ms) Process

Recommendation 6

We recommend that the Owners of ARRTS revise the POA&M items currently listed to include the recommendations, rather than just identifying the weaknesses.

Response 6

We concur with the recommendation and will implement the changes to the current POA&M items. As soon as ARRTS is transitioned to the OCIO, the ARRTS stakeholders will coordinate with the OCIO for remediation of the existing POA&Ms, tracking their progress, and adding new vulnerabilities as they are identified.

Recommendation 7

We recommend that the Owners of ARRTS develop a plan for the immediate remediation of all overdue POA&M items.

Response 7

We concur with the recommendation and will review the current POA&M items. As ARRTS is transitioned to the OCIO, the stakeholders will coordinate with the OCIO for the remediation of the existing POA&Ms.

AT-3 Security Training

Recommendation 8

We recommend that the Owners of ARRTS identify the individuals with significant information technology (IT) responsibility for ARRTS that require specialized IT security training.

Response 8

We concur with the recommendation and a list of individuals from the OIG that have significant IT responsibility for ARRTS will be compiled and those names will be supplied to the OCIO to ensure that these individuals receive specialized IT security training annually.

Recommendation 9

We recommend that the Owners of ARRTS ensure that all employees with significant information security responsibility for ARRTS take meaningful and appropriate specialized security training on an annual basis.

Response 9

We concur with the recommendation and the OIG will add a POA&M to the OIG LAN POA&Ms that requires the tracking of the annual security training for the all staff that has significant IT responsibilities. A report pertaining to the staff training will be provided to the OCIO.

The Owners of ARRTS' management of audit logs for ARRTS could be improved

Recommendation 10
We recommend that the Owners of ARRTS develop an audit policy that contains a list of events that should be logged for ARRTS at the database and application levels.

Response 10
We concur with the recommendation and the OCIO and the three stakeholders will develop an audit policy that contains a list of events that should be logged.

Recommendation 11
We recommend that the ARRTS system be modified to generate audit logs in accordance with audit policy and in compliance with all applicable NIST 800-53 standards.

Response 11
We concur with the recommendation and ARRTS will be evaluated for the feasibility of implementing system modifications to generate audit logs that are in compliance with NIST 800-53 standards.

Recommendation 12
We recommend that ARRTS be modified to ensure all audit logs cannot be inappropriately accessed, modified, or deleted.

Response 12
We concur with the recommendation and ARRTS will be evaluated for the feasibility of system modifications to ensure that audit logs cannot be inappropriately accessed, modified, or deleted.

Recommendation 13
We recommend that the Owners of ARRTS routinely monitor/review audit logs generated by ARRTS.

Response 13
We concur with the recommendation and procedures will be put in place to ensure that ARRTS audit logs are routinely monitored and reviewed.

IA-4 Identifier Management

Recommendation 14
We recommend that the Owners of ARRTS disable/delete unnecessary duplicate ARRTS user accounts.

Response 14
We concur with the recommendation however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. Access to the ARRTS system requires that a user first log into the OPM LAN with a valid user ID and password. If an OPM staff

member is terminated, retires, or leaves the agency they no longer have access to the OPM LAN and as a result they can no longer access the ARRTS application. If the employee changes jobs within OPM and no longer requires access to ARRTS, documented procedures will be in place to ensure that the ARRTS application is removed from that individual's computer. While there may be a low level risk still associated with outdated user IDs remaining active in ARRTS, we believe the level of risk is extremely low. This matter will require a Business Case Exception to be developed and approved to accept this risk.

Recommendation 15
We recommend that the Owners of ARRTS implement a process to routinely audit all active user accounts to ensure that no unnecessary duplicate accounts exist.

Response 15
We concur with the recommendation and will implement a process to routinely review all active user accounts in ARRTS however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. Access to the ARRTS system requires that a user first log into the OPM LAN with a valid user ID and password. If an OPM staff member is terminated, retires, or leaves the agency they no longer have access to the OPM LAN and as a result they can no longer access the ARRTS application. If the employee changes jobs within OPM and no longer requires access to ARRTS, documented procedures will be in place to ensure that the ARRTS application is removed from that individual's computer. While there may be a low level risk still associated with outdated user IDs remaining active in ARRTS, we believe the level of risk is extremely low. This matter will require a Business Case Exception to be developed and approved to accept this risk.

PS-4 Personnel Termination

Recommendation 16
We recommend that the Owners of ARRTS disable active user accounts that belong to terminated employees.

Response 16
We concur with the recommendation however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. Access to the ARRTS system requires that a user first log into the OPM LAN with a valid user ID and password. If an OPM staff member is terminated, retires, or leaves the agency they no longer have access to the OPM LAN and as a result they can no longer access the ARRTS application. If the employee changes jobs within OPM and no longer requires access to ARRTS, documented procedures will be in place to ensure that the ARRTS application is removed from that individual's computer. While there may be a low level risk still associated with outdated user IDs remaining active in ARRTS, we believe the level of risk is extremely low. This matter will require a Business Case Exception to be developed and approved to accept this risk.

Recommendation 17
We recommend that the Owners of ARRTS periodically audit active ARRTS user accounts to verify that accounts do not remain open for individuals no longer employed at OPM and that the level of access granted remains appropriate.

Response 17
We concur with the recommendation and will implement procedures requiring periodic audits of active ARRTS user accounts however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. Access to the ARRTS system requires that a user first log into the OPM LAN with a valid user ID and password. If an OPM staff member is terminated, retires, or leaves the agency they no longer have access to the OPM LAN and as a result they can no longer access the ARRTS application. If the employee changes jobs within OPM and no longer requires access to ARRTS, documented procedures will be in place to ensure that the ARRTS application is removed from that individual's computer. While there may be a low level risk still associated with outdated user IDs remaining active in ARRTS, we believe the level of risk is extremely low. This matter will require a Business Case Exception to be developed and approved to accept this risk.

PS-5 Personnel Transfer

Recommendation 18
We recommend that the Owners of ARRTS disable/delete unnecessary user IDs for users who no longer have a business reason to have access to ARRTS.

Response 18
We concur with the recommendation however, the ARRTS database design requires that the user ID that the record was stored under be present; removing or disabling any user ID makes any records that are associated with that user ID irretrievable. Access to the ARRTS system requires that a user first log into the OPM LAN with a valid user ID and password. If an OPM staff member is terminated, retires, or leaves the agency they no longer have access to the OPM LAN and as a result they can no longer access the ARRTS application. If the employee changes jobs within OPM and no longer requires access to ARRTS, documented procedures will be in place to ensure that the ARRTS application is removed from that individual's computer. While there may be a low level risk still associated with outdated user IDs remaining active in ARRTS, we believe the level of risk is extremely low. This matter will require a Business Case Exception to be developed and approved to accept this risk.

PS-6 Access Agreements

Recommendation 19
We recommend that the Owners of ARRTS develop a Rules of Behavior/Acceptable Use Statement for ARRTS and ensure it is signed by all users.

Response 19
We concur with the recommendation and the OIG will implement a Rules of Behavior/Acceptable Use document specifically for ARRTS to be signed by all current and future ARRTS users.

RA-5 Vulnerability Scanning

Recommendation 20
We recommend that the Owners of ARRTS ensure that routine vulnerability scans are conducted on the system.

Response 20
We concur with the recommendation and as soon as ARRTS is transitioned to the OCIO's LAN/WAN GSS, the OCIO plans to do routine vulnerability scans.

CM-6 Configuration Settings

Recommendations 21
We recommend that the database supporting ARRTS be configured in a manner that is compliant with OPM's policies.

Response 21
We concur with the recommendation and will coordinate with the OCIO to ensure that the database and server is configured in a manner that is compliant with OPM's policies.

Recommendation 22
We recommend that the server supporting ARRTS be configured in a manner that is compliant with OPM's policies.

Response 22
We concur with the recommendation will coordinate with the OCIO to ensure that ARRTS is compliant with OPM policies.

Classification of ARRTS as a Minor Application

Recommendation 23
We recommend that the Owners of ARRTS work with the OCIO to reclassify ARRTS as a minor application within the LAN/WAN general support system.

Response 23
We concur with the recommendation and a Memorandum of Understanding is being developed in anticipation of the downgrade of ARRTS to a minor application system and the transition of ARRTS to the OPM LAN/WAN GSS.

Recommendation 24
We recommend that the OCIO update the LAN/WAN Information System Security Plan (ISSP) to reflect ARRTS as a minor application.

Response 24
We concur with the recommendation and we are currently working with the OCIO to downgrade ARRTS to a minor application. We will work closely with the OCIO to ensure that the LAN/WAN ISSP is updated to reflect ARRTS as a minor application.

If you need any additional information or have any questions to our response to your draft audit report, please contact [redacted] at ([redacted], or [redacted], of my staff, at [redacted]

cc: [redacted]
Chief, Trust Funds
Office of the Chief Financial Officer

[redacted]
Chief, Audit Resolution
Healthcare and Insurance Office

[redacted]
Chief, Client Server Branch
Office of the Chief Information Officer

Terri Fazio
Assistant IG for Management
Office of the Inspector General

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

[redacted]
Deputy Director
Internal Oversight and Compliance