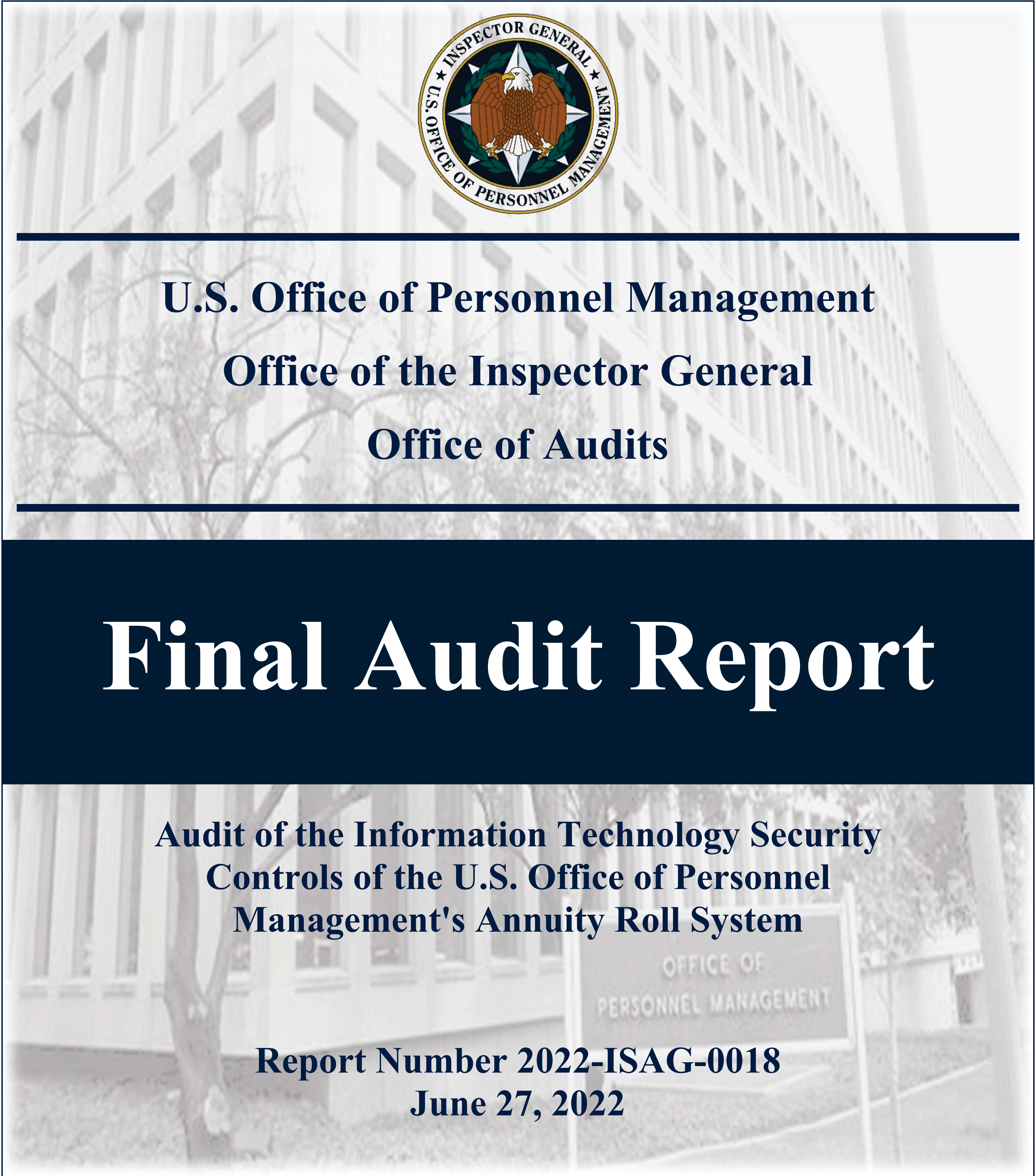

U.S. Office of Personnel Management

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 Annuity Roll System

Report Number 2022-ISAG-0018
June 27, 2022

Executive Summary

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

Report No. 2022-ISAG-0018 **June 27, 2022**

Why Did We Conduct the Audit?

The Annuity Roll System (ARS) is one of the U.S. Office of Personnel Management's (OPM) major information technology (IT) systems. The Federal Information Security Modernization Act (FISMA) requires that the Office of the Inspector General perform audits of IT security controls of agency systems.

What Did We Audit?

We completed a performance audit of ARS to ensure that the system's security controls meet the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual, 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 IT security controls of ARS determined that:

- A Security Assessment and Authorization was completed on February 17, 2021. The Authorization was granted for up to three years.
- The ARS security categorization is consistent with Federal Information Processing Standards 199, and we agree with the "moderate" categorization.
- OPM has completed a Privacy Impact Assessment and Privacy Threshold Analysis with an expiration date of January 2023.
- The ARS System Security Plan was complete and follows the OCIO's template.
- The OCIO performed a security assessment and has documented procedures and test cases.
- Continuous Monitoring for ARS was conducted in accordance with OPM's quarterly schedule for fiscal year 2021.
- The ARS contingency plan was completed in accordance with NIST Special Publication (SP) 800-34, Revision 1, and OCIO guidance.
- The ARS Plan of Action and Milestones documentation is up to date and contains all identified weaknesses.
- We evaluated a subset of the system controls outlined in NIST SP 800-53, Revision 4. We determined that the security controls tested appear to be in compliance.

Abbreviations

ARS	Annuity Roll System
ATO	Authorization to Operate
Authorization	Security Assessment and Authorization
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	U.S. Office of Management and Budget
OPM	U.S. Office of Personnel Management
PIA	Privacy Impact Assessment
POA&M	Plan of Action and Milestones
PTA	Privacy Threshold Analysis
SP	Special Publication
SSP	System Security Plan

Table of Contents

I. Background

On December 17, 2002, the President signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act. It requires (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) the results of Inspector General evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In 2014, Public Law 113-283, the Federal Information Security Modernization Act (FISMA) was established and reaffirmed the objectives of the prior Act.

The Annuity Roll System (ARS) has been included in this year's subset of systems because it is one of OPM's moderate risk, major systems, and an audit of its information technology (IT) security controls has not been conducted within the past 10 years. According to the ARS System Security Plan (SSP), ARS is a system that "contains the detailed records on annuitants and their survivors and forms the basic pay records for disbursing benefits" for Federal employees.

The OPM Office of the Chief Information Officer (OCIO) has responsibility for implementing and managing the IT security controls of ARS. We discussed the results of our audit with OPM representatives and provided a draft report to illicit their comments. As the draft report did not contain any formal recommendations, we only received technical comments in response. We appreciated the technical comments provided in response to the draft report, and we have implemented those comments within the final report.

All OPM personnel that worked with the auditors were helpful and open to ideas and suggestions. They viewed the audit as an opportunity to examine practices and to make changes or improvements as necessary. Their positive attitude and helpfulness throughout the audit was greatly appreciated.

II. Objective, Scope, and Methodology

Objective

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

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

- Security Assessment and Authorization;
- Federal Information Processing Standards Publication 199 (FIPS 199) Analysis;
- Privacy Impact Assessment;
- System Security Plan;
- Security Assessment Plan and Report;
- Continuous Monitoring;
- Contingency Planning and Contingency Plan Testing;
- Plan of Action and Milestones (POA&M) Process; and
- NIST Special Publication (SP) 800-53, Revision 4, Security Controls.

Scope and Methodology

We conducted this performance audit in accordance with the Generally Accepted 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 security controls and FISMA compliance efforts of OPM officials responsible for ARS, including the evaluation of IT security controls in place as of February 2022.

We considered the ARS 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 objective.

To accomplish our objective, we interviewed representatives of OPM's OCIO with security responsibilities for ARS, reviewed documentation and system screenshots, viewed demonstrations of system capabilities, and conducted tests directly on the system. We also 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.

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 during this audit caused us to doubt the reliability of the computer-generated data used. We believe that the data was sufficient to achieve the audit objectives.

Details of the security controls protecting the confidentiality, integrity, and availability of ARS are located in the "Audit Findings" 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 ARS internal controls taken as a whole. The criteria used in conducting this audit include:

- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- Public Law 113-283, Federal Information Security Modernization Act of 2014;
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Revision 1, Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems; and
- OMB's Circular A-130, Appendix I.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether OPM's management of ARS is consistent with applicable standards. We determined that OPM was mostly in compliance with all standards as described in Section III of this report, and any items that were not in compliance were previously identified in OPM's POA&M documentation.

III. Audit Findings

A. Security Assessment and Authorization

A Security Assessment and Authorization (Authorization) includes: 1) a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system and 2) an official management decision to authorize operation of an information system and accept its known risks. OMB's Circular A-130, Appendix I, mandates that all Federal information systems have a valid Authorization. Although OMB previously required periodic Authorizations every three years, Federal agencies now have the option of continuously monitoring their systems to fulfill the Authorization requirement. OPM does not yet have a mature program in place to continuously monitor system security controls; therefore, a current Authorization is required for all OPM systems at least once every three years as required by OPM policy.

OPM management granted ARS an authorization to operate (ATO) in February 2021. The ATO is valid for up to three years and includes provisions that the system owner monitor and remediate identified weaknesses on an ongoing basis.

ARS was granted an ATO in February 2021.

The ATO also requires that OPM assess and manage any significant system changes in accordance with OMB policies.

Nothing came to our attention to indicate that the ARS's ATO was inadequate.

B. FIPS 199 Analysis

The E-Government Act of 2002 requires Federal agencies to assign a security categorization to all Federal information and information systems. FIPS Publication 199 defined standards to be used by Federal agencies to categorize information systems based on appropriate levels of information security according to risk. Minimum information security requirements of each information system are determined based on the system's security categorization assigned using FIPS Publication 199 guidance.

NIST SP 800-60, Revision 1, Volume II, provides an overview of the security objectives and impact levels identified in FIPS 199.

The security categorization document includes an analysis of the information processed by the ARS and the corresponding impact of confidentiality, integrity, and availability. The ARS is categorized as a "moderate" impact level for each area – confidentiality, integrity, and availability – resulting in an overall categorization of "moderate."

The security categorization of the ARS appears to be consistent with FIPS 199 and NIST SP 800-60, Revision 1, Volume II requirements, and we agree with the categorization of "moderate." Additionally, the requirements of NIST SP 800-53, Revision 4, control RA-2 Security Categorization, have been adequately implemented.

No opportunities for improvement related to the ARS FIPS 199 security categorization were identified.

C. Privacy Impact Assessment

The E-Government Act of 2002 requires agencies to conduct a Privacy Impact Assessment (PIA) for systems that collect, maintain, or disseminate information that is in an identifiable form. The PIA should address privacy related concerns including, but not limited to, what information is to be collected; why the information is being collected; with whom the information will be shared; and how the information will be secured. A Privacy Threshold Analysis (PTA) documents the privacy risk and mitigation for the system and is used to determine whether a system requires a PIA.

The ARS Privacy Threshold Analysis and Privacy Impact Assessment are adequately documented.

In accordance with OPM policies requiring annual review, the ARS PTA was reviewed by OPM's Office of Privacy and Information Management in January 2022 and has an expiration date of January 2023. The analysis indicated that a PIA is required due to the sensitivity of the data maintained by the system.

OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system. In accordance with OMB and OPM requirements, the PIA was last updated and approved by the OPM Privacy Office in November 2021.

We did not detect any issues with the ARS PIA.

D. System Security Plan

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

The OCIO Retirement Services Information Technology Program Management Office developed the ARS SSP using the OCIO's SSP template which uses NIST SP 800-18, Revision 1, as guidance. The template requires the SSP to contain the following elements:

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

We reviewed the current ARS SSP, last updated in August 2021, and determined that it adequately reflects the system's current state. Nothing came to our attention to indicate that the ARS SSP has not been properly documented and approved.

E. Security Assessment Plan and Report

A Security Assessment Plan describes the scope, procedures, environment, team, roles, and responsibilities for an assessment to determine the effectiveness of a system's security controls. A Risk Assessment Report assesses the risk to the system for each weakness identified during the security controls assessment.

The ARS Security Assessment Plan was created by the OCIO Information System Security Officer (ISSO) in August 2013, and last updated in October 2020. The Risk Assessment Report was created by the OCIO ISSO in January 2021, and last updated in January 2022. OCIO has no existing POA&M related to the security assessment.

Nothing came to our attention to indicate that the ARS Security Assessment Plan or Report were inadequate.

F. Continuous Monitoring

OPM requires that the IT security controls of each system be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan that includes a template outlining the security controls that must be tested for all information systems. All system owners are required to tailor the Information Security Continuous

Monitoring Plan template to each individual system's specific security control needs and then test the system's security controls on an ongoing basis. The test results must be provided to the OCIO on a routine basis for centralized tracking.

We received the fiscal year 2021 quarterly continuous monitoring submissions for ARS. A review of the submissions revealed that 149 distinct controls were tested. We also received the quarter one fiscal year 2022 continuous monitoring submissions for ARS. A review of the submissions revealed that 76 distinct controls were tested.

Nothing came to our attention to indicate that ARS could not participate in an agency-wide Continuous Monitoring program.

G. 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.

1) Contingency Plan

The ARS contingency plan, approved in January 2021, documents the functions, operations, and resources necessary to restore and resume the system when unexpected events or disasters occur. The contingency plan also ensures coordination with external points of contact and vendors associated with ARS. The contingency plan follows the format suggested by NIST SP 800-34, Revision 1, and OPM's template for contingency plans.

We did not detect any issues with the ARS contingency plan.

2) Contingency Plan Testing

Contingency plan testing is a critical element of a viable disaster recovery capability. OPM requires that contingency plans for all systems be tested annually to evaluate the plan's effectiveness and the organization's readiness to execute the plan. NIST SP 800-34, Revision 1, provides guidance for testing contingency plans and documenting the results.

The contingency plan and test were completed in accordance with NIST guidance.

The ARS contingency plan test was conducted in August 2019. The test consisted of recovering and validating the ARS mainframe from an alternate location after a major disaster. The functional test was considered successful although there were issues with expired passwords during the testing process, and while lessons learned were documented and provided to the Authorizing Official, System Owner, and OPM CISO, the document has not been signed or approved in accordance with NIST guidance. There will not be a contingency plan test finding or recommendation in this report, as the program office has previously identified the issue and created a corresponding POA&M.

Nothing else came to our attention to indicate that the ARS contingency plan testing process was inadequate.

H. 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 known 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.

There are 17 open POA&Ms for ARS with issues identified that need to be remediated. The risk level for all the POA&Ms are medium with completion dates ranging from February 2022 to June 2022. The ARS POA&M is properly formatted according to OPM policy, and all weaknesses are properly documented to include attainable closure dates.

We did not detect any issues with the ARS POA&M.

I. NIST SP 800-53 Evaluation

NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the Federal government. As part of this audit, we tested a judgmental sample of NIST SP 800-53, Revision 4, controls. We chose a sample of 26 controls from a universe of 277 “moderate” controls. The sample included at least one control from each NIST control family. The judgmental sample was drawn from applicable controls that were identified in the latest security control assessment as “in place” and “system-specific.” The results of the judgmentally selected sample were not projected to the population since it is unlikely that the results are representative of the population. The controls that were examined were from each of the following control families:

- Access Control;
- Audit and Accountability;
- Awareness and Training;
- Configuration Management;
- Contingency Planning;
- Identity and Authentication;
- Incident Response;
- Media Protection;
- Planning;
- Risk Assessment;
- Security Assessment and Authorization;
- System and Communications Protection;
- System and Information Integrity; and
- System and Services Acquisition.

These controls were evaluated by interviewing individuals with system 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.

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