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 Federal Annuity Claims Expert System

Report Number 4A-RS-00-16-035
November 21, 2016

-- 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 Federal Annuity Claims Expert System

Report No. 4A-RS-00-16-035 **November 21, 2016**

Why Did We Conduct the Audit?

The Federal Annuity Claims Expert System (FACES) is one of the U.S. 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 FACES 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 Security 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 the IT security controls of FACES determined that:

- A Security Assessment and Authorization (SA&A) of FACES has not been completed in the last four years. We reviewed the most recent authorization package for all required elements of an SA&A, and determined that while the package does contain all necessary documentation, the majority of those documents are out of date.
- The security categorization of FACES is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60 requirements, and we agree with the categorization of "moderate."
- The FACES System Security Plan has not been updated to reflect the current control requirements of NIST.
- OPM has not performed adequate continuous monitoring of the security controls of the system for the last two years.
- A contingency plan was developed for FACES that is in compliance with NIST SP 800-34 Revision 1. However, the plan has not been tested annually.
- A privacy threshold analysis was conducted for FACES that indicated that a Privacy Impact Assessment (PIA) was required. However, a PIA has not been conducted since October 2012.
- The FACES 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, we noted several POA&M items that were over 200 days overdue and did not indicate a new scheduled completion date.
- We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 4 were implemented for the FACES. We determined that the majority of tested security controls appear to be in compliance with NIST SP 800-53 Revision 4. However, we did note several areas for improvement.

ABBREVIATIONS

FACES	**Federal Annuity Claims Expert System**
FIPS	**Federal Information Processing Standards**
FISMA	**Federal Information Security Management Act**
IG	**Inspector General**
ISCMP	**Information Security Continuous Monitoring Plan**
IT	**Information Technology**
NIST	**National Institute of 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 Analysis**
POA&M	**Plan of Action and Milestones**
RS	**Retirement Services**
Authorization	**Security Assessment and Authorization**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

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. It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the U.S. 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 2014, Public Law 113-283, the Federal Information Security Modernization Act (FISMA) was established and reaffirmed the objectives of the prior FISMA. As part of our evaluation, we will review the U.S. Office of Personnel Management (OPM)'s FISMA compliance strategy and document the status of their compliance efforts. In accordance with FISMA, we audited the information technology (IT) security controls related to OPM's Federal Annuity Claims Expert System (FACES).

FACES 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 FACES system is used to make calculations related to Federal retirement benefits. The system is comprised of a public facing web application used by Federal employees to estimate financial retirement information, and also an internal web application used by OPM's Retirement Services (RS) program office benefit officers for retirement-related computations.

This was our first audit of the security controls surrounding FACES. OPM's Office of the Chief Information Officer (OCIO) and RS share responsibility for implementing and managing the IT security controls of FACES. We discussed the results of our audit with OCIO and RS representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our objective was to perform an evaluation of the security controls for FACES to ensure that OCIO and RS 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 and OPM's OCIO.

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

- Security Assessment and Authorization (Authorization);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- System Security Plan (SSP);
- Continuous Monitoring;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment (PIA);
- Plan of Action and Milestones Process (POA&M); 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 for FACES, including the evaluation of IT security controls in place as of April 2016.

We considered the FACES 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 RS and OCIO program offices with FACES security responsibilities, 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.

Details of the security controls protecting the confidentiality, integrity, and availability of FACES 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 FACES' 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: The NIST Handbook;
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60, Revision 1, 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 Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with the 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 April 2016 through August 2016 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

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

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Assessment and Authorization

A Security Assessment and 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 III mandates that all Federal information systems have a valid Authorization. Although OMB previously required an Authorization to be performed every three years, Federal agencies now have the option of continuously monitoring their systems' IT security controls in lieu of performing formal Authorizations. However, OPM does not yet have a mature program in place to continuously monitor system security controls, and therefore we continue to expect a current Authorization to exist for every OPM system.

OPM's fiscal year 2015 FISMA report (4A-CI-00-15-011) includes a material weakness related to the agency's failure to meet OMB authorization requirements for many of its major information systems. FACES was one of the OPM systems contributing to this material weakness. The prior authorization for FACES expired in January 2015, and the system does not have a valid Authorization as of the date of this report.

Failure to properly authorize a major system means that the program office cannot properly manage, mitigate, or accept the security risks for the unauthorized system.

<u>Recommendation 1</u>

We recommend that OPM complete a current Security Assessment and Authorization for FACES.

<u>OPM Response:</u>

"Concur; steps have been taken to correct this. A Security Assessment and Authorization (SA&A) was initiated by the OPM Office of the Chief Information Security Officer (CISO) on 8/6/2016 for Federal Annuity Claim Expert System (FACES) system, as mandated by OMB's Circular A-130, Appendix III; following NIST 800-53A guidance for assessing federal IT systems. Security Assessment Plan is on track to be completed by September 30, 2016 and will be provided to the IG."

OIG Comment:

OPM submitted evidence that an Authorization for FACES is in progress, but it has not been completed as of the date of this report. As part of the audit resolution process, OPM should provide the Internal Oversight and Compliance (IOC) division with evidence that it has implemented this recommendation. This statement also applies to all subsequent recommendations in this report that OPM agrees to implement.

B. 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 FACES FIPS Publication 199 Security Categorization documentation analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. FACES is categorized with a moderate impact level for confidentiality, moderate for integrity, and moderate for availability – resulting in an overall categorization of moderate.

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

C. System Security Plan

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

The SSP for FACES was created using the OCIO's SSP template that utilizes NIST SP 800-18, Revision 1, as guidance. 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 FACES SSP and determined that it does not adequately address all of the requirements of NIST. Specifically, the most recent SSP for FACES does not include controls that were added to the current revision of NIST SP 800-53 (Revision 4).

NIST SP 800-53, Revision 4, was published in April 2013, and FIPS Publication 200 states that "Federal agencies will have up to one year from the date of final publication to fully comply with the changes but are encouraged to initiate compliance activities immediately."

Recommendation 2

We recommend that OPM update the FACES SSP in accordance with the agency's policies and NIST standards.

OPM Response:

"Non-Concur. As part of the current FACES SA&A ATO Relay initiative which started on 8/6/2016, the SSP was updated to add the most current revision of NIST SP 800-53 (Revision 4), in accordance with OPM Cybersecurity requirements. The SA&A control assessment are based on the most current NIST 800-53/800-53A standards. The updated Rev 4 SSP and SSP security control matrix is provided in this response."

OIG Comment:

Although OPM's response indicates that it does not concur with the recommendation, the evidence included with its response indicates that it has taken steps to update the SSP per our recommendation. However, the SSP provided does not document many of the controls required for this system. As part of the audit resolution process, we recommend that OPM provide IOC with additional evidence to show that all required controls have been implemented and that the FACES SSP has been completed and approved.

D. Continuous Monitoring

OPM requires that the IT security controls of each application be assessed on a continuous basis. OPM's OCIO has developed an Information Security Continuous Monitoring Plan (ISCMP) that includes a template outlining the security controls that must be tested for all information systems. This template must be tailored to each individual system's specific security control needs. All system owners are required to customize their system's ISCMP and then test the system's security controls according to the plan. The results of the testing must then be provided to the OCIO for centralized tracking every quarter.

We reviewed the FACES ISCMP test submissions from 2014 and 2015. The documentation for both years indicates that the FACES system was not subject to adequate security control testing in those years. Furthermore, our audit determined that there have not been any security control tests completed for FACES since April 2015.

Failure to perform continuous monitoring activities increases the risk that unknown vulnerabilities exist within the system that can be exploited.

Recommendation 3

We recommend that OPM ensure that the FACES security controls are continuously monitored in accordance with the agency's policy.

OPM Response:

"Concur; steps have been taken to correct this. As a condition for all OPM IT Systems receiving an Authority to Operate (ATO), participation in the OPM Information System Continuous Monitoring (ISCM) program is mandatory. This includes designated security control evaluation in accordance to the ISCM plan, provided to all OPM IT systems based on an SA&A and risk evaluation. Vulnerability scanning security control was completed for FACES during the week of August 15, 2016 and remediation plans have been identified and is provided in this response. Contingency Plan Test and After Action Report are also attached."

OIG Comment:

OPM's response to the draft report included vulnerability scan reports and remediation plans for FACES. While vulnerability scans are a critical aspect of continuous monitoring, the intent of this recommendation is to ensure that continuous monitoring is taking place for all security controls outlined in the ISCMP. This recommendation should not be closed until OPM provides evidence that the security controls of FACES are being tested in accordance with the ISCMP.

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

2) Contingency Plan Test

OPM requires that contingency plans be tested annually to determine 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. Contingency plan testing is a critical element of a viable disaster recovery capability.

The most recent contingency plan test we received for FACES was conducted in August 2014. This does not meet OPM's policy that requires contingency plans to be tested annually. Failure to adequately exercise the contingency plan could lead to an excessive outage time during an actual disaster recovery scenario.

Recommendation 4

We recommend that OPM perform a test of the FACES contingency plan and ensure annual testing in accordance with OPM policy and NIST SP 800-34, Revision 1, standards.

<u>OPM Response:</u>

"Concur; steps have been taken to correct this. As a condition for all OPM IT Systems receiving an Authority to Operate (ATO), all systems are required to test its contingency plan as required by OPM policy and NIST SP 800-34, Revision 1, standards. A Contingency Plan Test and After Action Report were completed on September 20, 2016. The results are attached."

<u>OIG Comment:</u>

In response to the draft audit report, OPM provided evidence that a contingency plan test was performed in the current year; no further action is required.

F. Privacy Impact Assessment

FISMA requires agencies to perform a screening of Federal information systems to determine if a PIA is required for that system. OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate and document any personally identifiable information maintained by an information system.

RS completed an initial privacy screening or Privacy Threshold Analysis of FACES and determined that a PIA was required for this system. The most recent PIA was conducted for FACES in October of 2012, and was appropriately based on the guidance contained in OPM's PIA Guide. However, OPM policy requires system owners to conduct a PIA every three years for existing systems even when there are no changes to the system.

<u>Recommendation 5</u>

We recommend that OPM ensure that a PIA is conducted for FACES in accordance with OPM policy.

<u>OPM Response:</u>

"Concur; steps have been taken to correct this. CSP is working with the OPM Privacy Officer to utilize recently updated and Privacy Threshold Analysis (PTA) and Privacy Impact Analysis (PIA) templates in completing this requirement. Preliminary PTA and PIA reports are attached."

OIG Comment:

In response to the draft audit report, OPM provided unsigned drafts of a PIA and PTA for FACES. As part of the audit resolution process, we recommend that OPM provide IOC with evidence of final and approved versions of these documents.

G. 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.

We evaluated the FACES POA&M and verified that it follows the format of OPM's standard template. However, we noted that 20 of the 25 items on the FACES POA&M were over 200 days overdue. We also determined that many of the security weaknesses discovered during continuous monitoring activities for FACES were not added to the system's POA&M.

The OPM POA&M Standard Operating Procedures states that "If the weakness is not addressed by the scheduled completion date, the new scheduled completion date must be addressed in the Milestone Changes column, along with the updated milestones and dates necessary to achieve the new scheduled completion date."

Failure to properly maintain a system's POA&M increases the likelihood of weaknesses not being addressed in a timely manner and therefore exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

Recommendation 6

We recommend that OPM add a POA&M entry for all known weaknesses of FACES.

OPM Response:

"Concur; steps have been taken to correct this. As a requirement of the SA&A package, a POA&M list of the known weaknesses of FACES will be provided and documented within the OPM IT Security repository system, as a provision for issuances of an ATO. In addition, the POA&M process will now include a POA&M board to ensure POA&Ms are maintained properly. Evidence is attached."

OIG Comment:

The POA&M provided by OPM in response to the draft audit report still did not contain many of the weaknesses identified from prior continuous monitoring submissions. This evidence does not address our concern that weaknesses identified from security control testing are not being tracked in the system's POA&M.

Recommendation 7

We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.

OPM Response:

"Concur; steps have been taken to correct this. As a requirement of the SA&A package, a POA&M list of the known weaknesses of FACES will be provided with resources and/or hours needed to mitigate the finding, documented within the OPM IT Security repository system, as a provision for issuance of an ATO. Evidence is attached."

OIG Comment:

The POA&M provided by OPM in response to the draft audit report lists scheduled completion dates that are the same for all weaknesses even though the weaknesses vary greatly in complexity. The intent of our recommendation is to develop a reasonable action plan and schedule to remediate the existing FACES POA&M items that are overdue.

H. 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 evaluated whether a subset of these controls had been implemented for FACES.

We tested approximately 44 controls as outlined in NIST SP 800-53, Revision 4, including 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;
- Identity and Authentication;
- Incident Response;
- Maintenance;
- Media Protection;

- Physical and Environmental Protection;
- Planning;
- Personnel Security;
- Risk Assessment;
- System and Services Acquisition;
- System and Communications Protection; and
- System and Information Integrity.

These controls were evaluated by interviewing individuals with FACES 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 AC-22 – Publicly Accessible Content

We discovered sensitive personally identifiable information available on the public facing portion of the FACES website. This information was available on a page that did not require any sort of authentication to access. This audit report will not discuss the details of what data was found or where it was located, but this information was provided directly to the OCIO and RS. The OCIO and RS promptly removed this information from the FACES website after we notified them of the issue.

Recommendation 8

We recommend that OPM implement a process to routinely review the FACES website to ensure that sensitive information is not publically available.

OPM Response:

"Concur; steps have been taken to correct this. Evidence is attached."

OIG Comment:

OPM's response to the draft audit report did not contain any evidence related to this recommendation. As part of the audit resolution process, OPM should provide IOC with evidence that it has implemented this recommendation.

2) Control CA-3 – System Interconnections

The SSP states that FACES does not have any system interconnections. However, our analysis of this system architecture indicates that FACES is not a standalone system and is, in fact, directly connected to at least two of OPM's other major information systems.

OPM's Information Security and Privacy Policy Handbook states that "If both systems are owned by the organization MOUs and/or ISAs are not required, but the interface characteristics between systems shall be documented in the respective SSPs."

It is critical to identify all of a system's interconnections so that the security risks associated with the interconnections can be appropriately managed.

Recommendation 9

We recommend that OPM update the FACES SSP to document the system's interconnection characteristics, security requirements, and the nature of the information communicated between FACES and other systems.

OPM Response:

Concur; steps have been taken to correct this. The ISSO reviewed the SSP and identified that information sharing text was documented outside of the information share table. SSP was updated on September 21, 2016, in the Appendix I section, to show information sharing test within the Information sharing table. Evidence is attached."

OIG Comment:

The intent of this recommendation is to ensure that the connections between information systems are appropriately documented. The privacy impact assessment states that data is passed between FACES and two other systems through a system interface. However, the SSP does not acknowledge these as system interconnections. This recommendation should not be closed without evidence that the connections have been documented appropriately or that it is has been demonstrated that FACES does not have any dedicated connections to other systems.

3) Control IA-2 Identification and Authentication

The FACES system can be accessed via a username and password; there are no requirements to use multi-factor authentication. OMB Memorandum M-11-11 requires all major information systems to enforce multi-factor authentication using PIV cards. This issue is being tracked in an existing OIG audit recommendation (Report No. 4A-CI-00-15-011, Recommendation 16). Although we will not issue a duplicate recommendation in this report, it is critical that FACES be modified to require multi-factor authentication via PIV cards as soon as possible.

4) Control IA-5 Authenticator Management

The vulnerability scans we performed on the FACES system indicated that the operating system authentication settings for several of the [redacted] servers supporting the application did not comply with OPM authentication requirements. The specific settings will not be detailed in this audit report, but the information was provided directly to RS and OCIO personnel.

Failure to implement strong authentication standards increases the organization's risk to brute force password attacks that could compromise the system and associated accounts.

Recommendation 10

We recommend that OPM ensure that all FACES servers comply with OPM authentication standards.

OPM Response:

"Concur; this concern is resolved. A meeting was held on September 22, 2016 with SMEs to discuss the resolution of this finding. Evidence is attached."

OIG Comment:

The evidence that was provided in response to the draft audit report relates to the use of PIV cards for accessing OPM *workstations*. We continue to recommend that RS and OCIO provide IOC with evidence that all FACES *servers* are in compliance with OPM authentication standards, and that they cannot be accessed by an account not managed by the external identity management solution.

5) Control SC-7 – Boundary Protection

FACES is comprised of three major components: 1) the main application server; 2) backend databases; and 3) a web application that allows users to access the system from the public Internet.

[redacted]

[redacted]

Recommendation 11

[redacted]

OPM Response:

"Concur; steps have been taken to correct this. A meeting was held on September 22, 2016 with SMEs to discuss the resolution of this finding. Evidence is attached."

OIG Comment:

The evidence provided in response to the draft report indicates OPM is developing a plan to implement this recommendation, but no concrete solution is currently in place. As part of the audit resolution process, OPM should provide IOC with evidence when it has fully implemented this recommendation.

6) [redacted]

[redacted]

[redacted]

<u>Recommendation 12</u>

[redacted]

<u>OPM Response:</u>

"Concur; steps have been taken to correct this. A meeting was held on September 22, 2016 with SMEs to discuss the resolution of this finding. A PO&AM will be created to address this finding. Evidence is attached."

<u>OIG Comment:</u>

The evidence provided in response to the draft report indicates that this recommendation cannot be implemented until [redacted]. As part of the audit resolution process, OPM should provide IOC with evidence when it has fully implemented this recommendation.

7) Control SI-2 – Flaw Remediation

An information system flaw is a vulnerability resulting from inherent and known IT security weaknesses. These flaws are typically remediated through software updates such as patches, service packs, hot fixes, and anti-virus signature updates. Information system flaws may be identified through various processes and controls such as security control assessments, continuous monitoring, and routine vulnerability scanning activities.

There are many individuals in both RS and the OCIO with some form of responsibility for addressing security flaws on the FACES system. However, during the course of the audit, we had difficulty identifying the appropriate OCIO and RS personnel to discuss how various security controls were implemented for FACES. It became apparent that there are not clearly defined roles and responsibilities for those tasked with managing IT security and remediating security flaws for this system. For example, we saw evidence that automated vulnerability scans were routinely run against the system, but did not see evidence that: 1) the scan results were routed to the individuals that have the authority and ability to fix the flaw; or 2) that any individual was tracking the known flaws to ensure that they were addressed in a timely manner.

The vulnerability scans that we performed as part of this audit detected numerous security flaws that have existed in the FACES system for a long time (multiple years, in some cases). We believe that this is a direct result of the lack of formal accountability regarding the management of IT security for this system.

NIST SP 800-53, Revision 4, requires that organizations identify, report, and correct information system flaws. NIST SP 800-115 states that “Verification can take place by conducting an audit of the system, retesting the system and its components, and holding personnel accountable through documentation.”

Failure to properly track the resolution of system flaws could leave systems exposed to known vulnerabilities.

Recommendation 13

We recommend that OPM document the roles and responsibilities associated with system security for the FACES system. This should include the identification of specific individuals responsible for remediating specific types of system flaws (e.g., missing server patches, application code weaknesses, database vulnerabilities, etc.) and individuals responsible for verifying that flaws have been addressed.

OPM Response:

“Concur; steps have been taken to address this. ISSO met with FACES SMEs during week of September 19, 2016 and the SSP was updated on September 19, 2016 that identifies specific individuals responsible for remediating specific types of system flaw (e.g., missing server patches, application code weakness, database vulnerabilities) and individuals responsible for verifying that flaws have been addressed. The Rev 4 SSP is updated in section 2.8.3 to show roles and responsibilities associated with system security for the FACES system. Evidence is attached.”

OIG Comment:

In response to the draft audit report, OPM provided evidence that responsibilities for ensuring that flaws are remediated have been defined and documented in the SSP; no further action is required.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge
[redacted], Lead IT Auditor
[redacted], IT Auditor

[redacted], Group Chief

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANEGEMENT
Washington, DC 20415

September 26, 2016

MEMORANDUM FOR [redacted]
Chief, Information Systems Audit Group
Office of the Inspector General

FROM: DAVID De VRIES
Chief Information Officer

KENNETH ZAWODNY
Associate Director
Retirement Services

SUBJECT: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Federal Annuity Claims Expert System (Report No. 4A-RS-00-16-035)

Thank you for providing us the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Federal Annuity Claims Expert System, Report No. 4A-RS-00-16 - 035.

We recognize that even the most well run programs benefit from evaluations and we appreciate your input as we continue to enhance our programs. Our responses to your recommendations are provided in the attachment below.

Attachment:

cc: Cord Chase
Chief Information Security Officer

Mark W. Lambert
Associate Director, Merit System Audit and Compliance

Janet Barnes
Director, Internal Oversight and Compliance

OPM Response to OIG Draft Report
Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Federal Annuity Claims Expert System (Report No. 4A-RS-00-16-035)

Recommendation 1:
We recommend that OPM complete a current Security Assessment and Authorization for FACES.

Management Response:
Concur; steps have been taken to correct this. A Security Assessment and Authorization (SA&A) was initiated by the OPM Office of the Chief Information Security Officer (CISO) on 8/6/2016 for Federal Annuity Claim Expert System (FACES) system, as mandated by OMB's Circular A-130, Appendix III; following NIST 800-53A guidance for assessing federal IT systems. Security Assessment Plan is on track to be completed by September 30, 2016 and will be provided to the IG.

Recommendation 2:
We recommend that OPM update the FACES SSP in accordance with the agency's policies and NIST standards.

Management Response:
Non-Concur. As part of the current FACES SA&A ATO Relay initiative which started on 8/6/2016, the SSP was updated to add the most current revision of NIST SP 800-53 (Revision 4), in accordance with OPM Cybersecurity requirements. The SA&A control assessment are based on the most current NIST 800-53/800-53A standards. The updated Rev 4 SSP and SSP security control matrix is provided in this response.

Recommendation 3:
We recommend that OPM ensure that the FACES security controls are continuously monitored in accordance with the organization policy.

Management Response:
Concur; steps have been taken to correct this. As a condition for all OPM IT Systems receiving an Authority to Operate (ATO), participation in the OPM Information System Continuous Monitoring (ISCM) program is mandatory. This includes designated security control evaluation in accordance to the ISCM plan, provided to all OPM IT systems based on an SA&A and risk evaluation. Vulnerability scanning security control was completed for FACES during the week of August 15, 2016 and remediation plans have been identified and is provided in this response. Contingency Plan Test and After Action Report are also attached.

Recommendation 4:
We recommend that OPM perform a test of the FACES contingency plan and ensure annual testing in accordance with OPM policy and NIST SP 800-34, Revision 1, standards.

Management Response:
Concur; steps have been taken to correct this. As a condition for all OPM IT Systems receiving an Authority to Operate (ATO), all systems are required to test its contingency plan as required by OPM policy and NIST SP 800-34, Revision 1, standards. A Contingency Plan Test and After Action Report were completed on September 20, 2016. The results are attached.

Recommendation 5:
We recommend that OPM ensure that a PIA is conducted for FACES in accordance with OPM policy.

Management Response:
Concur; steps have been taken to correct this. CSP is working with the OPM Privacy Officer to utilize recently updated and Privacy Threshold Analysis (PTA) and Privacy Impact Analysis (PIA) templates in completing this requirement. Preliminary PTA and PIA reports are attached.

Recommendation 6:
We recommend that OPM add a POA&M entry for all known weaknesses of FACES.

Management Response:
Concur; steps have been taken to correct this. As a requirement of the SA&A package, a POA&M list of the known weaknesses of FACES will be provided and documented within the OPM IT Security repository system, as a provision for issuance of an ATO. In addition, the POA&M process will now include a POA&M board to ensure POA&Ms are maintained properly. Evidence is attached.

Recommendation 7:
We recommend that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.

Management Response:
Concur; steps have been taken to correct this. As a requirement of the SA&A package, a POA&M list of the known weaknesses of FACES will be provided with resources and/or hours needed to mitigate the finding, documented within the OPM IT Security repository system, as a provision for issuance of an ATO. Evidence is attached.

Recommendation 8:
We recommend that OPM implement a process to routinely review the FACES website to ensure that sensitive information is not publically available.

Management Response:
Concur; steps have been taken to correct this. Evidence is attached.

Recommendation 9:
We recommend that OPM update the FACES SSP to document the system's interconnection characteristics, security requirements, and the nature of the information communicated between FACES and other systems.

Management Response:
Concur; steps have been taken to correct this. The ISSO reviewed the SSP and identified that information sharing text was documented outside of the information sharing table. SSP was updated on September 21, 2016, in the Appendix I section, to show information sharing text within the Information sharing table. Evidence is attached.

Recommendation 10:
We recommend that OPM ensure that all FACES servers comply with OPM authentication standards.

Management Response:
Concur; this concern is resolved. A meeting was held on September 22, 2016 with SMEs to discuss the resolution of this finding. Evidence is attached.

Recommendation 11:
[redacted]

Management Response:
Concur; steps have been taken to correct this. A meeting was held on September 22, 2016 with SMEs to discuss the resolution of this finding. Evidence is attached.

Recommendation 12:
[redacted]

Management Response:
Concur; steps have been taken to correct this. A meeting was held on September 22, 2016 with SMEs to discuss the resolution of this finding. A PO&AM will be created to address this finding. Evidence is attached.

Recommendation 13:
We recommend that OPM document the roles and responsibilities associated with system security for the FACES system. This should include the identification of specific individuals responsible for remediating specific types of system flaws (e.g., missing server patches, application code weaknesses, database vulnerabilities, etc.) and individuals responsible for verifying that flaws have been addressed

Management Response:
Concur; steps have been taken to address this. ISSO met with FACES SMEs during week of September 19, 2016 and the SSP was updated on September 19, 2016 that identifies specific individuals responsible for remediating specific types of system flaw (e.g., missing server patches, application code weakness, database vulnerabilities) and individuals responsible for verifying that flaws have been addressed. The Rev 4 SSP is updated in section 2.8.3 to show roles and responsibilities associated with system security for the FACES system. Evidence is attached.

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