



---

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

---

# Open Recommendations

**Open Recommendations Over Six Months Old as of  
September 30, 2018**

**November 30, 2018**



# EXECUTIVE SUMMARY

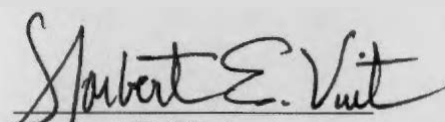
*Open Recommendations Over Six Months Old as of  
September 30, 2018*

November 30, 2018

## Why Did We Prepare This Report?

Under the Inspector General Act of 1978, as amended by the Inspector General Empowerment Act of 2016, each Office of the Inspector General (OIG) is required to include in its Semiannual Report to Congress certain information related to outstanding recommendations. These reporting requirements were inspired by prior standing requests for information submitted to all OIGs by the Senate Committee on Homeland Security and Governmental Affairs, the House Committee on Oversight and Government, and Senator Charles Grassley.

This report was prepared to both fulfill the OIG's reporting obligation under the Inspector General Act as well as to continue providing the previously-requested information to Congress.

  
Norbert E. Vint  
Acting Inspector General

As of September 30, 2018, there were 310 outstanding recommendations contained in reports that the OIG had issued to the U.S. Office of Personnel Management over six months old.

Type of Report	# of Reports	Total # Recs. Made	# Open Recs. as of 9/30/18
Internal Audits	24	173	110
Information Systems Audits	23	361	170
Experience-Rated Health Insurance Audits	8	64	18
Community-Rated Health Insurance Audits	1	2	2
Other Insurance Audits	2	7	2
Evaluations	2	6	5
Management Advisories	1	3	3
<b>Total</b>	<b>61</b>	<b>616</b>	<b>310</b>

Below is a chart showing the number of open procedural and monetary recommendations for each report type:

Type of Report	Procedural	Monetary	Value of Monetary Recs.*
Internal Audits	109	1	\$108 million
Information Systems Audits	170	0	\$0
Experience-Rated Health Insurance Audits	9	9	\$99.5 million
Community-Rated Health Insurance Audits	0	2	\$3.6 million
Other Insurance Audits	1	1	\$812,800
Evaluations	5	0	\$0
Management Advisories	3	0	\$0
<b>Total</b>	<b>297</b>	<b>13</b>	<b>\$211.9 million</b>

\*Totals are rounded.

# ABBREVIATIONS

<b>AFR</b>	<b>Annual Financial Report</b>
<b>BCBS</b>	<b>BlueCross BlueShield</b>
<b>BIA</b>	<b>Business Impact Analysis</b>
<b>CBIS</b>	<b>Consolidated Business Information System</b>
<b>CFCS</b>	<b>Combined Federal Campaign System</b>
<b>CISO</b>	<b>Chief Information Security Officer</b>
<b>CM</b>	<b>Configuration Management</b>
<b>COB</b>	<b>Coordination of Benefits</b>
<b>CPIC</b>	<b>Capital Planning and Investment Control</b>
<b>GSA</b>	<b>General Services Administration</b>
<b>FAR</b>	<b>Federal Acquisition Regulation</b>
<b>FEHBP</b>	<b>Federal Employees Health Benefits Program</b>
<b>FEP</b>	<b>BCBS's Federal Employee Program</b>
<b>FERS</b>	<b>Federal Employees Retirement System</b>
<b>FFS</b>	<b>Federal Financial System</b>
<b>FISMA</b>	<b>Federal Information Security Management Act</b>
<b>FSAFEDS</b>	<b>Federal Flexible Spending Account Program</b>
<b>FY</b>	<b>Fiscal Year</b>
<b>HCSC</b>	<b>Health Care Service Corporation</b>
<b>HMO</b>	<b>Health Maintenance Organization</b>
<b>HRS</b>	<b>Human Resources Solutions</b>
<b>IPERA</b>	<b>Improper Payments Elimination and Recovery Act</b>
<b>ICAM</b>	<b>Identity, Credential, and Access Management</b>
<b>IRS</b>	<b>Internal Revenue Service</b>
<b>ISCM</b>	<b>Information Security Continuous Monitoring</b>
<b>ISSO</b>	<b>Information System Security Officer</b>
<b>IT</b>	<b>Information Technology</b>
<b>LII</b>	<b>Lost Investment Income</b>
<b>LOB</b>	<b>Line of Business</b>
<b>N/A</b>	<b>Not Applicable</b>
<b>NIST</b>	<b>National Institute of Standards and Technology</b>
<b>OBRA 90</b>	<b>Omnibus Budget Reconciliation Act of 1990</b>
<b>OCFO</b>	<b>Office of the Chief Financial Officer</b>
<b>OCIO</b>	<b>Office of the Chief Information Officer</b>
<b>OIG</b>	<b>Office of the Inspector General</b>
<b>OPM</b>	<b>U.S. Office of Personnel Management</b>
<b>OPO</b>	<b>Office of Procurement Operations</b>
<b>PBM</b>	<b>Pharmacy Benefit Manager</b>
<b>PIA</b>	<b>Privacy Impact Assessment</b>
<b>PII</b>	<b>Personally Identifiable Information</b>
<b>PIV</b>	<b>Personal Identity Verification</b>
<b>POA&amp;M</b>	<b>Plan of Action and Milestones</b>
<b>PPO</b>	<b>Preferred Provider Organization</b>
<b>RRB</b>	<b>Railroad Retirement Board</b>
<b>RS</b>	<b>Retirement Services</b>
<b>RSM</b>	<b>Retirement System Modernization</b>

<b>SAA</b>	<b>Security Assessment and Authorization</b>
<b>SDLC</b>	<b>System Development Life Cycle</b>
<b>SSA</b>	<b>Social Security Administration</b>
<b>SSP</b>	<b>System Security Plan</b>
<b>SSSG</b>	<b>Similarly Sized Subscriber Group</b>
<b>TAS</b>	<b>Treasury Account Symbol</b>
<b>VA</b>	<b>U.S. Department of Veterans Affairs</b>

# TABLE OF CONTENTS

	<u>Page</u>
ABBREVIATIONS .....	i
I. INTERNAL AUDITS .....	1
II. INFORMATION SYSTEMS AUDITS .....	46
III. EXPERIENCE-RATED HEALTH INSURANCE AUDITS .....	99
IV. COMMUNITY-RATED HEALTH INSURANCE AUDITS .....	108
V. OTHER INSURANCE AUDITS .....	109
VI. EVALUATIONS .....	111
VII. MANAGEMENT ADVISORIES .....	114
APPENDIX: LIST OF ALL REPORTS WITH OPEN RECOMMENDATIONS .....	115

# I. INTERNAL AUDITS

This section describes the open recommendations from audits conducted by the Internal Audits Group. This group conduct audits of internal OPM programs and operations.

<b>Title: Audit of the Fiscal Year 2008 Financial Statements</b>		
<b>Report #: 4A-CF-00-08-025</b>		
<b>Date: November 14, 2008</b>		
<b>Rec. #</b>		
1	<b><i>Finding</i></b>	<u>Information Systems General Control Environment</u> –Security policies and procedures have not been updated to incorporate current authoritative guidance and the procedures performed to certify and accredit certain financial systems were not complete. In addition, it was noted that application access permissions have not been fully documented to describe the functional duties the access provides to assist management in reviewing the appropriateness of system access. Also, there were instances where background investigations and security awareness training was not completed prior to access being granted.
	<b><i>Recommendation</i></b>	The OCIO should continue to update and implement entity-wide security policies and procedures and provide more direction and oversight to Program Offices for completing certification and accreditation requirements. In addition, documentation on application access permissions should be enhanced and linked with functional duties and procedures for granting logical access need to be refined to ensure access is granted only to authorized individuals.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

**Title: Audit of the Fiscal Year 2009 Financial Statements**

**Report #: 4A-CF-00-09-037**

**Date: November 13, 2009**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems General Control Environment</u> – Information system general control deficiencies identified in previous years related to OPM and its programs continue to persist or have not been fully addressed and consequently are not in full compliance with authoritative guidance.
	<b>Recommendation</b>	KPMG recommends that the Office of the Chief Information Officer should continue to update and implement entity-wide policies and procedures and provide more direction and oversight to Program Offices for completing and appropriately overseeing certification and accreditation requirements and activities. In addition, documentation on application access permissions should be enhanced and linked with functional duties and procedures for granting logical and physical access needs to be refined to ensure access is granted only to authorized individuals. Finally, policies and procedures should be developed and implemented to ensure POA&Ms are accurate & complete.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

**Title: Audit of the Fiscal Year 2010 Financial Statements**

**Report #: 4A-CF-00-10-015**

**Date: November 10, 2010**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems General Control Environment</u> – Deficiencies in OPM's and the Programs' information system general controls that were identified and reported as a significant deficiency in previous years continue to persist. Although changes in information system management during this fiscal year, including the appointment of a new Chief Information Officer (CIO) and Senior Agency Information Security Officer, have resulted in plans to address these weaknesses, these plans have not yet been fully executed to resolve long-standing deficiencies in OPM's security program.
	<b>Recommendation</b>	KPMG recommends that the CIO develop and promulgate entity-wide security policies and procedures and assume more responsibility for the coordination and oversight of Program Offices in completing certification and accreditation and other information security requirements and activities.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

*Continued: Audit of the Fiscal Year 2010 Financial Statements*

2	<b>Finding</b>	<u>Information Systems General Control Environment</u> – See number 1 above.
	<b>Recommendation</b>	KPMG recommends that the CIO identify common controls, control responsibilities, boundaries and interconnections for information systems in its system inventory.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
3	<b>Finding</b>	<u>Information Systems General Control Environment</u> – See number 1 above
	<b>Recommendation</b>	KPMG recommends that the CIO implement a process to ensure the POA&Ms remain accurate and complete.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

**Title: Stopping Improper Payments to Deceased Annuitants**

**Report #: 1K-RS-00-11-068**

**Date: September 14, 2011**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Tracking of Undeliverable IRS Form 1099Rs</u> – OPM does not track undeliverable IRS Form 1099Rs to determine if any annuitants in the population of returned 1099Rs could be deceased.
	<b>Recommendation</b>	The OIG recommends that OPM annually track and analyze returned Form 1099Rs for the prior tax year. Performing this exercise provides OPM with the opportunity to identify deceased annuitants whose death has not been reported; continue to update the active annuity roll records with current address information; and to correct other personal identifying information. In addition, the returned Form 1099Rs should be matched against the SSA Death Master File annually.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	Potentially significant detection of and reduction in improper payments.
	<b>Other Nonmonetary Benefit</b>	Updated annuity roll records.



*Continued: Stopping Improper Payments to Deceased Annuitants*

<b>Rec. #</b>		
2	<b><i>Finding</i></b>	<u>Capitalizing on RSM Technology</u> – A modernized environment offers opportunities to reduce instances of fraud, waste, and abuse of the retirement trust fund.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM actively explore the capabilities of any automated solution to flag records and produce management reports for anomalies or suspect activity, such as multiple address or bank account changes in a short time.
	<b><i>Status</i></b>	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved detection of potential improper payments.
3	<b><i>Finding</i></b>	<u>Establishment of Working Groups to Improve Program Integrity</u> – Under the Office of Management and Budget’s Circular A-123, Management’s Responsibility for Internal Control, OPM has the responsibility to design controls to protect the integrity of program data. OPM cannot carry out this responsibility effectively unless it is continually reviewing and analyzing data from the active annuity roll and related sources to identify potential weaknesses and flaws in its operations and programs.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM form a group comprised of “Subject Matter Experts” to explore risk areas and develop computer programs to look for anomalies that could indicate possible fraud.  To further this effort, OPM should also establish a working group with other benefit-paying agencies, such as the VA, SSA, RRB, and the Department of Health and Human Services to determine best practices, keep up-to-date on the latest internal controls, and share/match death information.
	<b><i>Status</i></b>	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved detection of potential improper payments.

**Title: Audit of the Fiscal Year 2011 Financial Statements**  
**Report #: 4A-CF-00-11-050**  
**Date: Audit of the Fiscal Year 2011 Financial Statements**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	<b>Recommendation</b>	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to address the information system control environment weaknesses.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

**Title: Audit of the Fiscal Year 2012 Financial Statements**  
**Report #: 4A-CF-00-12-039**  
**Date: Audit of the Fiscal Year 2012 Financial Statements**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	<b>Recommendation</b>	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to address the information system control environment weaknesses.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

**Title: Audit of OPM's Voice over Internet Protocol Interagency Agreement**  
**Report #: 1K-RS-00-12-031**  
**Date: December 12, 2012**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Expense Documentation not Maintained</u> : After several attempts, OPM was unable to provide invoices documenting actual incurred contract expenses.  While the D.C. Government is responsible for documenting all contract related charges, OPM has a responsibility to review and maintain this documentation to ensure that all funds are appropriately accounted for and that <u>only appropriate charges are being invoiced against OPM's contract</u> .
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to ensure that all VoIP agreement invoices are fully supported, thereby providing assurance that they are for services consistent with the terms of OPM's agreement with the D.C. Government.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls over the financial aspects of intergovernmental agreements when buying goods and services.

**Title: Audit of OPM's Fiscal Year 2013 Financial Statements**  
**Report #: 4A-CF-00-13-034**  
**Date: December 13, 2013**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	<b>Recommendation</b>	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to address the information system control environment weaknesses.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

**Title: Audit of OPM's Fiscal Year 2014 Financial Statements**  
**Report #: 4A-CF-00-14-039**  
**Date: November 10, 2014**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	<b>Recommendation</b>	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to implement the current authoritative guidance regarding two-factor authentication.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
2	<b>Finding</b>	<u>Information Systems Control Environment</u> - Access rights in OPM systems are not documented and mapped to personnel roles and functions to ensure that personnel access is limited only to the functions needed to perform their job responsibilities.
	<b>Recommendation</b>	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to document and map access rights in OPM systems to personnel roles and functions, following the principle of "least privilege."
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

*Continued: Audit of OPM's Fiscal Year 2014 Financial Statements*

3	<b>Finding</b>	<p><u>Information Systems Control Environment</u> - The information security control monitoring program was not fully effective in detecting information security control weaknesses. We noted access rights in OPM systems were:</p> <ul style="list-style-type: none"> <li>• Granted to new users without following the OPM access approval process and quarterly reviews to confirm access approval were not consistently performed.</li> <li>• Not revoked immediately upon user separation and quarterly reviews to confirm access removal were not consistently performed.</li> </ul>
	<b>Recommendation</b>	<p>KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to enhance OPM's information security control monitoring program to detect information security control weakness by:</p> <ul style="list-style-type: none"> <li>• Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process.</li> <li>• Monitoring the process for the identification and removal of separated users to ensure that user access is removed timely upon separation; implementing procedures to ensure that user access, including user accounts and associated roles, are reviewed on a periodic basis consistent with the nature and risk of the system, and modifying any necessary accounts when identified.</li> </ul>
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

**Title: Audit of OPM's Compliance with the Freedom of Information Act**

**Report #: 4K-RS-00-14-076**

**Date: March 23, 2015**

<b>Rec. #</b>		
1	<b>Finding</b>	<p><u>Compliance with Electronic Freedom of Information Act Amendments of 1996 (E-FOIA)</u> - OPM's FOIA policy does not discuss the requirement to post information online that has been requested multiple times. In addition, OPM's request tracking system does not identify the type of information requested. Consequently, OPM's FOIA Office cannot identify multiple requests that should be posted.</p>
	<b>Recommendation</b>	The OIG recommends that OPM's FOIA Office document a formal policy for handling multiple requests of the same information.
	<b>Status</b>	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing FOIA information requests.

*Continued: Audit of OPM's Compliance with the Freedom of Information Act*

3	<b><i>Finding</i></b>	Compliance with <u>Electronic Freedom of Information Act Amendments of 1996</u> : E-FOIA requires agencies to provide online reading rooms for citizens to access records and, in the instance of three or more requests for certain FOIA information that this information be posted in these rooms. OPM's website has a reading room that OPM's FOIA Office can use to post responses to multiple requests; however, we found that the reading room is not used.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM's FOIA Office start tracking types of FOIA requests to help determine whether they are multiple requests that must be posted to the reading room.
	<b><i>Status</i></b>	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for managing FOIA information requests.

**Title: Assessing the Internal Controls over OPM's Retirement Services Retirement Eligibility and Services Office**

**Report #: 4A-RS-00-13-033**

**Date: April 13, 2015**

<b>Rec. #</b>		
1	<b><i>Finding</i></b>	<u>Federal Employees Retirement System Annuity Supplement Surveys and Matches Not Completed</u> - RS has not conducted the 2013 FERS Annuity Supplement Survey and has not performed an annual Annuity Supplement Match since 2009.
	<b><i>Recommendation</i></b>	The OIG recommends that RS strengthen its internal controls over the FERS Annuity Supplement Survey and Match processes to ensure that benefit payments are made only to eligible annuitants, and FERS Annuity Surveys and Matches are conducted annually to implement the required annual reductions to benefits, as required by 5 U.S.C. 8421a.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over the annuity supplement surveys and matches process, it will increase OPM's effectiveness in ensuring that benefit payments are made only to eligible annuitants, thereby decreasing the number of improper payments.

**Title: Audit of Human Resources Solutions' Pricing Methodologies**  
**Report #: 4A-HR-00-13-055**  
**Date: June 2, 2015**

<b>Rec. #</b>		
5	<b>Finding</b>	<u>Prices for FY 2013 and 2014 Services Were Not Fully Supported</u> - One out of six Training and Management Assistance Program (TMAP) projects sampled did not have documentation to support the project costs (i.e., costing tools and interagency agreements). TMAP stated that they created this project in error. TMAP provided a Consolidated Business Information System screenshot that stated the project is "in progress"; however, there was no confirmation that the project was cancelled.
	<b>Recommendation</b>	The OIG recommends that HRS strengthen its internal controls to ensure that projects are properly reviewed and approved to prevent projects created in error.
	<b>Status</b>	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and corrective actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place to ensure proper review and approval of HRS projects, then the risk of customer agencies being under- or over-charged will decrease.

**Title: Audit of OPM's Fiscal Year 2015 Financial Statements**  
**Report #: 4A-CF-00-15-027**  
**Date: November 13, 2015**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems Control Environment</u> - The current authoritative guidance regarding two-factor authentication has not been fully applied.
	<b>Recommendation</b>	KPMG recommends that the OCIO fully implement the current authoritative guidance regarding two-factor authentication.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

*Continued: Audit of OPM's Fiscal Year 2015 Financial Statements*

2	<b>Finding</b>	<u>Information Systems Control Environment</u> - Access rights in OPM systems are not documented and mapped to personnel roles and functions to ensure that personnel access is limited only to the functions needed to perform their job responsibilities.
	<b>Recommendation</b>	KPMG recommends that the OCIO document and map access rights in OPM systems to personnel roles and functions, following the principle of “least privilege”.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
3	<b>Finding</b>	<u>Information Systems Control Environment</u> - The information security control monitoring program was not fully effective in detecting information security control weaknesses. We noted access rights in OPM systems were: <ul style="list-style-type: none"> <li>• Granted to new users without following the OPM access approval process and quarterly reviews to confirm access approval were not consistently performed.</li> <li>• Not revoked immediately upon user separation and quarterly reviews to confirm access removal were not consistently performed.</li> <li>• Granted to a privileged account without following the OPM access approval process.</li> </ul>
	<b>Recommendation</b>	KPMG recommends that the OCIO enhance OPM’s information security control monitoring program to detect information security control weaknesses by: <ul style="list-style-type: none"> <li>• Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process; and</li> <li>• Monitoring the process for the identification and removal of separated users to ensure that user access is removed timely upon separation; implementing procedures to ensure that user access, including user accounts and associated roles, are reviewed on a periodic basis consistent with the nature and risk of the system, and modifying any necessary accounts identified.</li> </ul>
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



*Continued: Audit of OPM's Fiscal Year 2015 Financial Statements*

4	<b>Finding</b>	A formalized system component inventory of devices to be assessed as part of vulnerability or configuration management processes was not maintained.
	<b>Recommendation</b>	KPMG recommends that the OCIO continue to perform, monitor, and improve its patch and vulnerability management processes, to include maintaining an accurate inventory of devices.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
5	<b>Finding</b>	<u>Entity Level Controls Over Financial Management</u> - During FY 2015 OPM reported a data breach which affected millions of Federal employees and government contractors. Based on KPMG's procedures to evaluate the potential impact of the data breach on OPM's financial statements, KPMG noted a number of control deficiencies that are pervasive throughout the agency.
	<b>Recommendation</b>	KPMG recommends that the OCFO perform a thorough review of OPM's entity-level controls over financial reporting and relevant activities to identify the underlying cause of these deficiencies and take the appropriate corrective actions to strengthen controls to mitigate risk of material misstatement when non-routine events occur.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Continued improvement in entity-level controls over financial management may improve the effectiveness of OPM's response to non-routine events and transactions and enhance the likelihood of the timely detection and correction of material misstatements in the financial statements.

**Title: Special Review of OPM’s Award of a Credit Monitoring and Identity Theft Services Contract to Winvale Group LLC, and its Subcontractor, CSIdentity**  
**Report #: 4K-RS-00-16-024**  
**Date: December 12, 2015**

Rec. #		
1	<b>Finding</b>	<p><u>Incomplete Statement of Work</u> - The OIG determined that the performance work statement for this contract award included the scope, period and place of performance, background, and performance objectives. However, the performance work statement was missing measurable performance standards and the method of assessing contractor performance. Therefore, the contracting officer did not ensure the performance work statement met the FAR requirements.</p> <p><u>Inadequate Market Research and Failure to Use a Small Business Specialist</u> – The OIG determined that the contracting officer inappropriately concluded that the market research was sufficient and did not require further analysis by a small business specialist.</p> <p><u>Inconclusive Determination on the use of GSA 's Federal Supply Schedule</u> – The OIG concluded that the contracting officer did not submit the Requirements to the GSA representative because an award through GSA would have caused the OCIO's Requirements due date to be missed.</p> <p><u>Lack of an Independent Government Cost Estimate</u> - We were informed by the contracting officer that an independent government cost estimate was not requested from the OCIO because meeting the OCIO's Requirements due date took precedence. In addition, we determined that the contracting officer did not obtain estimated costs from vendors during market research.</p> <p><u>Incomplete Acquisition Plan</u> – The OIG was informed by the contracting officer that the acquisition plan was drafted prior to the contract award; however, we were unable to verify when the acquisition plan was prepared. In addition, we determined that the acquisition plan was not approved by a higher level official above the contracting officer prior to the contract award on June 2, 2015.</p> <p><u>Blanket Purchase Agreement Call Exceeded FAR Limitation</u> - The contracting officer issued a blanket purchase agreement call order on June 2, 2015, in the amount of \$7,792,113 .88, which exceeded the FAR blanket purchase agreement limitation of \$6.5 million for individual purchases of a commercial item acquisition.</p> <p><u>Unreliable Contract File</u> - We were unable to obtain an accurate history of the actions taken by the contracting officer because key documents, specifically, the market research plan, acquisition plan, and System for Award Management support, were not prepared until after the contract award.</p>
	<b>Recommendation</b>	The OIG recommends that OPO immediately update its policies and procedures, to include but not be limited to, guidance for contract document approvals, emergency acquisitions, and contract file completion to ensure compliance with the FAR. When completed, contracting staff should be notified of the changes.
	<b>Status</b>	The agency agreed with the recommendation. OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If effective policies and procedures are in place then it will help ensure contracting officers are safeguarding the interests of the United States in its contractual relationship.

<i>Continued: Special Review of OPM's Award of a Credit Monitoring and Identity Theft Services Contract to Winvale Group LLC, and its Subcontractor, CSIdentity</i>		
2	<b><i>Finding</i></b>	See number 1 above for description.
	<b><i>Recommendation</i></b>	The OIG recommends that OPO implement controls to ensure that each contract is in compliance with the FAR requirements and contracting actions are documented and approved prior to contract award.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM has submitted evidence to the OIG for closure review.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If effective controls are in place to ensure the contract is in compliance, it will increase the likelihood that OPM is obtaining a qualified vendor.

<b>Title: Audit of OPM's Fiscal Year 2015 Improper Payments Reporting</b>		
<b>Report #: 4A-CF-00-16-026</b>		
<b>Date: May 11, 2016</b>		
<b>Rec. #</b>		
1	<b><i>Finding</i></b>	<b><i>Improper Payment Estimates' Root Causes:</i></b> The OIG found that OPM did not properly categorize the root causes of the retirement benefits program's improper payments in Table 13 of OPM's FY 2015 Agency Financial Report.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM implement controls to identify and evaluate the improper payment estimates root causes, to ensure that the root causes for the retirement benefits program's improper payments are properly categorized in OPM's annual Agency Financial Report.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place to identify the retirement services benefit programs improper payments estimates root cause, it will provide more granularity on the improper payment estimates, thus leading to more effective corrective actions at the program level and more focused strategies for reducing improper payments.

**Title: Audit of OPM's Office of Procurement Operations' Contract Management Process**

**Report #: 4A-CA-00-15-041**

**Date: July 8, 2016**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>OPO Lacks Strong Internal Controls Over Its Contract Management Operations</u> - On April 23, 2015, Calyptus issued its Strategic Assessment Report to OPO, which identified 16 recommendations for OPO. We reviewed Calyptus' Strategic Assessment Report of OPO and supporting documentation, and determined that the findings and recommendations reported by Calyptus are valid and logical. However, OPM is not ensuring that OPO takes appropriate corrective action to address the internal control deficiencies identified.
	<b>Recommendation</b>	The OIG recommends that OPO strengthen its internal controls by working with OPM's Internal Oversight and Compliance office to implement corrective actions to address the findings and recommendations reported in the Strategic Assessment Report issued by Calyptus Consulting Group, Inc., on April 23, 2015.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are free from deficiencies.
2	<b>Finding</b>	<u>Inaccurate Contract Amounts Reported in OPM's Information Systems</u> - We requested access to 60 contract files with open obligations reported in the OCFO's CBIS Fiscal Years 2010 to 2014 Open Obligation Report, and determined that the contract amounts reported in the Consolidated Business Information System (CBIS) for 22 of the 60 contracts sampled differed from the contract amounts reported in OPO's contract files. In addition, OPO was unable to provide 17 of the 60 contract files, so we cannot determine if the amounts reported in CBIS were accurate.
	<b>Recommendation</b>	The OIG recommends that OPO implement internal controls to ensure that contract data, including contract award amounts, is accurately recorded in OPM's information systems, such as CBIS, and the appropriate supporting documentation is maintained.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are appropriately reported in OPM's financial management system.

*Continued: Audit of OPM's Office of Procurement Operations' Contract Management Process*

3	<b>Finding</b>	<u>Weak Controls over the Contract Closeout Process</u> - OPO could not provide a listing of contract closeouts for FY 2013 and FY 2014. In addition, of the 60 contracts the OIG sampled, we identified 46 in which OPO did not initiate the contract closeout process in compliance with the FAR.
	<b>Recommendation</b>	The OIG recommends that OPO develop an accurate inventory of FYs 2013 and 2014 contracts ready for closeout.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.
4	<b>Finding</b>	<u>Weak Controls over the Contract Closeout Process</u> - See number 3 above.
	<b>Recommendation</b>	The OIG recommends that OPO establish and implement management controls to ensure that contracts are tracked and managed through the closeout process and adequate documentation is maintained in the contract file, including evidence of contract completion and closeout.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.
5	<b>Finding</b>	<u>Weak Controls over the Contract Closeout Process</u> - See number 3 above.
	<b>Recommendation</b>	The OIG recommends that OPO provide documentation to verify that the closeout process has been administered on the open obligations for the 46 contracts questioned.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.

<i>Continued: Audit of OPM's Office of Procurement Operations' Contract Management Process</i>		
6	<b>Finding</b>	<u>Weak Controls over the Contract Closeout Process</u> : As a result of the control deficiencies identified for the contract closeout process, as well as the issues previously discussed, we cannot determine if \$108,880,417 in remaining open obligations, associated with 46 questioned contracts, are still available for use by OPM's program offices.
	<b>Recommendation</b>	The OIG recommends that OPM's Office of Procurement Operations return \$108,880,417 in open obligations, for the 46 contracts questioned, to the program offices if support cannot be provided to show that the contract should remain open and the funds are still being utilized.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	\$108,880,417
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.

<u>Title: Audit of OPM's Fiscal Year 2016 Financial Statements</u>		
<u>Report #: 4A-CF-00-16-030</u>		
<u>Date: November 14, 2016</u>		
<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Systems Control Environment</u> : The Information Security and Privacy Policy Handbook is outdated.
	<b>Recommendation</b>	Grant Thornton recommends that OPM review, update, and approve the security management policies and procedures at the organization defined frequency. Updates should incorporate current operational procedures and removal of outdated procedures and terminology.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Policies will reflect current operational environment, which will allow personnel to develop and adhere to authorized processes and related controls.

*Continued: Audit of OPM's Fiscal Year 2016 Financial Statements*

2	<b>Finding</b>	<u>Information Systems Control Environment</u> : OPM System Documentation is outdated.
	<b>Recommendation</b>	Grant Thornton recommends that OPM create and/or update system documentation as follows: <ul style="list-style-type: none"> <li>• System Security Plans – Update the plans and perform periodic reviews in accordance with the organization defined frequencies.</li> <li>• Risk Assessments – Conduct a risk assessment for financially relevant applications and systems and a document comprehensive results of the testing performed.</li> <li>• Authority to Operate – Perform security assessment and authorization reviews in a timely manner and create up-to-date packages for systems.</li> <li>• Information System Continuous Monitoring – Document results of continuous monitoring testing performed for systems.</li> </ul>
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Complete and consistent security control documentation and complete and thorough testing will allow the agency to be informed of security control weaknesses that threaten the confidentiality, integrity, and availability of the data contained within its systems.
3	<b>Finding</b>	<u>Information Systems Control Environment</u> : The FISMA Inventory Listing is incomplete.
	<b>Recommendation</b>	Grant Thornton recommends that OPM enhance processes in place to track the inventory of the Agency's systems and devices.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	With an updated FISMA Inventory Listing, Management can: (a) work towards FISMA compliance, (b) develop an understanding of how transactions/data flow between the various systems, and (c) understand the totality of operational systems/applications within its environment.

*Continued: Audit of OPM's Fiscal Year 2016 Financial Statements*

4	<b>Finding</b>	<u>Information Systems Control Environment</u> : OPM lacks a system generated listing of terminated agency contractors.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement a system/control that tracks terminated contractors.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	A listing of terminated contractors to be reconciled against systems access will decrease the risk that users retain lingering access to systems and therefore will decrease the risk of inaccurate, invalid, and unauthorized transactions being processed by systems that could ultimately impact financial reporting.
5	<b>Finding</b>	<u>Information Systems Control Environment</u> : Role based training has not been completed.
	<b>Recommendation</b>	Grant Thornton recommends that OPM establish a means of documenting a list of users with significant information system responsibility to ensure the listing is complete and accurate and the appropriate training is completed.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Individuals obtain skills / training needed to perform day to day duties.
7	<b>Finding</b>	<u>Information Systems Control Environment</u> : Lack of Monitoring of Plan of Actions and Milestones (POA&Ms)
	<b>Recommendation</b>	Grant Thornton recommends that OPM assign specific individuals with overseeing/monitoring POA&Ms to ensure they are addressed in a timely manner.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The agency is able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.



*Continued: Audit of OPM's Fiscal Year 2016 Financial Statements*

8	<b>Finding</b>	<u>Information Systems Control Environment</u> : Lack of periodic access recertifications.
	<b>Recommendation</b>	Grant Thornton recommends that OPM perform a comprehensive review of the appropriateness of personnel with access to systems at the Agency's defined frequencies.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	A comprehensive review of personnel with access to the in-scope applications /systems will decrease the risk that inappropriate individuals maintain access allowing them to perform incompatible functions or functions associated with elevated privileges.
10	<b>Finding</b>	<u>Information Systems Control Environment</u> : [REDACTED], [REDACTED] are not PIV-compliant.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement two-factor authentication at the application level in accordance with agency and federal policies.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Two factor authentication will decrease the risk of unauthorized access into OPM systems.
11	<b>Finding</b>	<u>Information Systems Control Environment</u> : Lack of access descriptions and Segregation of Duties (SoD) Matrices.
	<b>Recommendation</b>	Grant Thornton recommends that OPM document access rights to systems to include roles, role descriptions, and privileges / activities associated with each role and role or activity assignments that may cause a segregation of duties conflict.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	A comprehensive understanding of user access rights will decrease the risk that users perform incompatible duties or have access to privileges or roles outside of what is needed to perform their day-to-day duties.

*Continued: Audit of OPM's Fiscal Year 2016 Financial Statements*

12	<b>Finding</b>	<u>Information Systems Control Environment</u> : Access procedures for terminated users are not followed.
	<b>Recommendation</b>	Grant Thornton recommends that OPM ensure termination processes (e.g., return of PIV badges and IT equipment, completion of Exist Clearance Forms and completion of exit surveys) are followed in a timely manner and documentation of completion of these processes is maintained.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Ensuring proper termination procedures are followed will decrease the risk that individuals gain / retain unauthorized access to IT resources/systems.
14	<b>Finding</b>	<u>Information Systems Control Environment</u> : The FACES audit logs are not periodically reviewed.
	<b>Recommendation</b>	Grant Thornton recommends that OPM review audit logs on a pre-defined periodic basis for violations or suspicious activity and identify individuals responsible for follow-up or evaluation of issues to the Security Operations Team for review. The review of audit logs should be documented for record retention purposes.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	A thorough review of audit logs decreases the risk that suspicious activity that occurs may go undetected and therefore may not be addressed in a timely manner.
15	<b>Finding</b>	<u>Information Systems Control Environment</u> : OPM lacks configuration management policies governing changes to the mainframe environment.
	<b>Recommendation</b>	Grant Thornton recommends that OPM establish a comprehensive configuration management plan that includes roles, responsibilities, and outlines details supporting authorization, testing, and documentation requirements.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Decreases the risk that unauthorized or erroneous changes to the mainframe configuration may be introduced without detection by system owners.

*Continued: Audit of OPM's Fiscal Year 2016 Financial Statements*

16	<b>Finding</b>	<u>Information Systems Control Environment</u> : OPM is unable to generate a complete and accurate listing of modifications to the mainframe and midrange environments.
	<b>Recommendation</b>	Grant Thornton recommends that OPM system owners establish a methodology to systematically track all configuration items that are migrated to production, and be able to produce a complete and accurate listing of all configuration items for both internal and external audit purposes, which will in turn support closer monitoring and management of the configuration management process.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Decreases the risk that unauthorized or erroneous changes to the mainframe and midrange configuration may be introduced without detection by system owners.
17	<b>Finding</b>	<u>Information Systems Control Environment</u> : OPM lacks a security configuration checklist
	<b>Recommendation</b>	Grant Thornton recommends that OPM enforce existing policy requiring mandatory security configuration settings, developed by OPM or developed by vendors or federal agencies, are implemented and settings are validated on a periodic basis to ensure appropriateness.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Restrictive security settings in place for components and a periodic assessment to ensure that such settings are in place and appropriate decreases the risk that the confidentiality, integrity, and / or availability of financial data is compromised.
19	<b>Finding</b>	<u>Monitoring Internal Controls</u> : A-123 Management's Responsibility for Internal Control
	<b>Recommendation</b>	Grant Thornton recommends that OPM strengthen the annual internal assessments, testing, and documentation based on OMB A-123, Appendix A guidance.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	N/A

**Title: Audit of OPM's Fiscal Year 2016 Improper Payments Reporting**  
**Report #: 4A-CF-00-17-012**  
**Date: May 11, 2017**

<b>Rec. #</b>		
10	<b>Finding</b>	<p><b>Improper Payment Root Causes:</b> Retirement Services was unable to fully categorize the following improper payments root causes in Table 2, "<i>Improper Payment Root Cause Category Matrix</i>," of the FY 2016 AFR: Federal employees retirement system's disability offset for social security disability, delayed reporting of eligibility, unauthorized dual benefits or overlapping payments between benefit paying agencies, and fraud.</p> <p>In the FY 2016 AFR, OPM acknowledges that they are aware of the major contributors of improper payments but are unable to provide the level of granularity needed to fully fulfill OMB Circular A-136 requirements. As a result, the remaining balance of these improper payments were placed in "Other Reason."</p>
	<b>Recommendation</b>	<p>The OIG recommends that OPM continue to implement controls to identify and evaluate the improper payment estimates root causes, to ensure that the root causes for the retirement benefits program's improper payments are properly categorized in OPM's annual AFR. <b>(Rolled-Forward from FY 2015)</b></p>
	<b>Status</b>	<p>The agency did not agree with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	<p>If controls are in place to identify the retirement services benefit programs improper payments estimates root cause, it will provide more granularity on the improper payment estimates, thus leading to more effective corrective actions at the program level and more focused strategies for reducing improper payments</p>

**Title: Audit of OPM's Purchase Card Program**

**Report #: 4A-OO-00-16-046**

**Date: July 7, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Cancellation of Purchase Cards</u> : OPO did not immediately cancel purchase cards when an employee separated from the agency. Of the 164 active purchase cards in OPM at the time of our audit, we found that 23, which had been issued to a former agency program coordinator, <sup>1</sup> were not immediately canceled when the employee separated from OPM on April 3, 2012.
	<b>Recommendation</b>	The OIG recommends that OPO perform verification and validation activities, such as utilizing available agency employee separation reports, to ensure that separated employees' purchase cards are immediately cancelled.
	<b>Status</b>	OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.
2	<b>Finding</b>	<u>Agency Financial Report (AFR)</u> : OPO could not provide documentation to support the \$238,400 outstanding balance reported in Table 19 - Purchase Cards, in the FY 2015 AFR.
	<b>Recommendation</b>	We recommend that OPO improve policies and procedures over its purchase card reporting process to ensure that data is supported and accurately reported.
	<b>Status</b>	OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.
3	<b>Finding</b>	<u>Agency Financial Report</u> : See number 2 above.
	<b>Recommendation</b>	We recommend that the OCFO verify and validate purchase card information prior to reporting it in the AFR to ensure the integrity of the data reported.
	<b>Status</b>	OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.

---

<sup>1</sup> OPM's normal practice is to issue one purchase card per cardholder. In this instance, the agency program coordinator was issued 23 purchase cards that were for 23 different program offices within OPM to be used for purchases that exceeded the \$3,500 micro-purchase limit.

*Continued: Audit of OPM's Purchase Card Program*

4	<b><i>Finding</i></b>	<p><u>Statistical Reporting</u>: OPO's FY 2016, third quarter (April 1 through June 30, 2016) statistical report is incomplete. We found that 2 out of 16 requirements were not reported. Specifically, OPO did not report the:</p> <ul style="list-style-type: none"> <li>• Number of purchase cardholders with contracting warrants above \$3,500, and</li> <li>• Number of purchase cardholders with transaction limits of \$3,500 or more that do not hold contracting warrants.</li> </ul>
	<b><i>Recommendation</i></b>	The OIG recommends that OPO immediately ensure that all OMB statistical reporting requirements are met, starting with their FY 2017 third quarter statistical report.
	<b><i>Status</i></b>	OPM has submitted evidence to the OIG for closure review.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.
5	<b><i>Finding</i></b>	<u>Statistical Reporting</u> : See number 4 above.
	<b><i>Recommendation</i></b>	The OIG recommends that OPO develop and implement policies and procedures for creating the quarterly OMB statistical report. At a minimum, the policies and procedures should include a discussion of all the statistical data elements required by OMB.
	<b><i>Status</i></b>	OPM has submitted evidence to the OIG for closure review.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.

*Continued: Audit of OPM's Purchase Card Program*

6	<b>Finding</b>	<u>Merchant Category Codes</u> : We found that OPO had not blocked, in JPMorgan Chase's PaymentNet, seven merchant category codes <sup>2</sup> for items that were restricted <sup>3</sup> or prohibited <sup>4</sup> from being purchased with a Government purchase card. We analyzed all 14,867 transactions, totaling \$7,969,765, from October 1, 2015, through June 30, 2016, and found that none of the restricted and prohibited codes were processed during the scope of the audit.
	<b>Recommendation</b>	The OIG recommends that OPO strengthen its oversight over merchant category codes accessible by purchase cardholders, to include developing and implementing policies and procedures for performing periodic reviews of merchant category codes, and eliminating cardholder's access to all restricted and prohibited codes from JPMorgan Chase's PaymentNet banking system.
	<b>Status</b>	OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.
7	<b>Finding</b>	<u>Training</u> : We randomly selected 61 out of 139 purchase card program participants to determine if initial and refresher training requirements were met. Specifically, we found that: <ul style="list-style-type: none"> <li>• 3 out of 61 purchase card program participants completed GSA SmartPay Purchase Account Agency Program Coordinator instead of the GSA SmartPay Account Holder training as refresher training.</li> <li>• 10 out of 61 purchase card program participants did not have documentation to support completion of training.</li> <li>• 23 out of 61 purchase card program participants completed initial training <i>after</i> being appointed as a purchase card program participant, or refresher training more than three years after the last refresher training.</li> </ul>
	<b>Recommendation</b>	The OIG recommends that OPO have all three purchase card program participants that took the GSA SmartPay Purchase Account Agency Program Coordinator training course immediately take the GSA SmartPay Account Holder training course or suspend their oversight duties until training is completed.
	<b>Status</b>	OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.

<sup>2</sup> Merchant category codes are established by the card issuing bank and are assigned to vendors as a means to identify the merchant type. Each cardholder account is set up with default merchant category codes that will allow the processing of transactions that fall under the specified merchant category code. If a transaction is attempted with any merchant that is categorized by a merchant category code blocked by OPO, the transaction will be electronically denied at the point of attempted purchase.

<sup>3</sup> Restricted items are those that can only be purchased with an Agency Program Coordinator authorized override.

<sup>4</sup> Prohibited items are those that cannot be purchased with a Government purchase card.

*Continued: Audit of OPM's Purchase Card Program*

8	<b><i>Finding</i></b>	<u>Training</u> : See number 7 above.
	<b><i>Recommendation</i></b>	The OIG recommends that OPO implement controls to ensure that purchase card program participants receive all required training on the appropriate use, controls, and consequences of abuse before appointment to their position, and receive refresher training every three years. Documentation should be maintained to support the completion of initial and refresher training.
	<b><i>Status</i></b>	OPM has submitted evidence to the OIG for closure review.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.
9	<b><i>Finding</i></b>	<u>Training</u> : See number 7 above.
	<b><i>Recommendation</i></b>	The OIG recommends that OPO suspend purchase card accounts and oversight duties of purchase card program participants that are not in compliance with refresher training requirements.
	<b><i>Status</i></b>	OPM has submitted evidence to the OIG for closure review.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.
10	<b><i>Finding</i></b>	<u>Controls over Purchase Card Transactions</u> : Controls over purchase card transactions, such as transaction documentation retention, and reallocating and approving transactions in OPM's financial system, need improvement to reduce the risk of fraud, waste, and abuse.
	<b><i>Recommendation</i></b>	The OIG recommends that OPO ensure that cardholders and/or program offices maintain documentation supporting transactions in accordance with purchase card policies and procedures.
	<b><i>Status</i></b>	OPM has submitted evidence to the OIG for closure review.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.



*Continued: Audit of OPM's Purchase Card Program*

11	<b>Finding</b>	<u>Controls over Purchase Card Transactions</u> : See number 10 above.
	<b>Recommendation</b>	The OIG recommends that OPO strengthen its oversight and monitoring of purchase card transactions, to include but not limited to, verifying that transactions are reallocated by cardholders and approved by approving officials in OPM's financial system.
	<b>Status</b>	OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.
12	<b>Finding</b>	<u>Controls over Purchase Card Transactions</u> : See number 10 above.
	<b>Recommendation</b>	The OIG recommends that that OPO provide documentation for the 17 unsupported transactions identified in Tables 2, 3, and 4.
	<b>Status</b>	OPM has submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over the purchase card program, it will increase OPM's effectiveness in reducing the risk of fraud, waste, and abuse related to government transactions.

**Title: Audit of the U.S. Office of Personnel Management's Data Submission and Compliance with the Digital Accountability and Transparency Act**  
**Report #: 4A-CF-00-17-033**  
**Date: November 9, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Summary-Level Differences between Data Submission Files A and B</u> : OPM's gross outlay amount by program object class in File B did not agree to the gross outlay amount by Treasury Account Symbol (TAS) in File A, and the obligations incurred by program object class in File B did not agree to obligations incurred by total in TAS.
	<b>Recommendation</b>	The OIG recommends that the OCFO continue to work with the CBIS Helpdesk to address calculation difference root cause(s) and provide categorical explanations for the misalignments between File A (appropriation summary level data) and File B (obligation and outlay information at program activity and object class level) prior to the FY 2019 DATA Act audit.
	<b>Status</b>	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If controls are in place over OPM's DATA Act submission and compliance, it will lead to increased data accuracy.

*Continued: Audit of OPM's Data Submission and Compliance with the Digital Accountability and Transparency Act*

2	<b><i>Finding</i></b>	<u>Lack of Effective and Efficient Standard Operating Procedures and Control Activities over the Data Submission Process</u> : The OCFO has a policy and procedures in place documenting their data submission process; however, they were unable to provide documentation to support that the policy and procedures were approved by the OCFO's Financial Operations Management division and communicated to the responsible Data Element Components, which consist of representatives from the offices of Procurement, Budget, Financial System, and Accounting.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCFO establish controls to ensure that DATA Act standard operating procedures are approved by management, documented, and communicated to the appropriate staff members prior to implementation and/or revision of any new or existing management directives.
	<b><i>Status</i></b>	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over OPM's DATA Act submission and compliance, it will lead to a more consistent process.
3	<b><i>Finding</i></b>	<u>Lack of Effective and Efficient Controls over Data Submission Files A through F</u> : The OCFO submitted OPM's DATA Act information by the end of the second quarter of FY 2017, and validated the accuracy of the data populated in Files A through C. However, the OCFO's internal controls did not include ensuring the interconnectivity/linkages across all data Files, A through F, to be displayed on USASpending.gov.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCFO establish controls to ensure that Files A through F are valid, reliable, accurate, and complete as required by OMB M-17-04.
	<b><i>Status</i></b>	The agency partially agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	If controls are in place over OPM's DATA Act submission and compliance, it will lead to increased data accuracy.

**Title: Audit of OPM's Fiscal Year 2017 Financial Statements**  
**Report #: 4A-CF-00-17-028**  
**Date: November 13, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	System Security Plans, Risk Assessments, Security Assessment and Authorization Packages and Information System Continuous Monitoring documentation were incomplete.
	<b>Recommendation</b>	Grant Thornton recommends that OPM review, update and approve policies and procedures in accordance with frequencies prescribed by OPM policy.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Policies will reflect current operational environment, which will allow personnel to develop and adhere to authorized processes and related controls.
2	<b>Finding</b>	OPM did not have a centralized process in place to maintain a complete and accurate listing of systems and devices to be able to provide security oversight or risk mitigation to the protection of its resources.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement processes to update the FISMA inventory listing to include interconnections, and review the FISMA inventory listing on a periodic basis for completeness and accuracy.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	With an updated FISMA Inventory Listing, Management can: (a) work towards FISMA compliance, (b) develop an understanding of how transactions/data flow between the various systems, and (c) understand the totality of operational systems/applications within its environment.
3	<b>Finding</b>	OPM did not have a centralized process in place to maintain a complete and accurate listing of systems and devices to be able to provide security oversight or risk mitigation to the protection of its resources.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement processes to associate software and hardware assets to system boundaries.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Complete and consistent security control documentation and complete and thorough testing will allow the agency to be informed of security control weaknesses that threaten the confidentiality, integrity, and availability of the data contained within its systems.

*Continued: Audit of OPM's Fiscal Year 2017 Financial Statements*

4	<b>Finding</b>	Instances of applications not scanned during the first quarter of FY 2017 and in July 2017 were noted.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement backup procedures to ensure continuous security scans over web applications.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Complete and consistent security control documentation and complete and thorough testing will allow the agency to be informed of security control weaknesses that threaten the confidentiality, integrity, and availability of the data contained within its systems.
5	<b>Finding</b>	OPM did not have a system in place to identify and generate a complete and accurate listing of OPM contractors and their employment status.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement a system or control that tracks the employment status of OPM contractors.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	A listing of contractors to be reconciled against systems access will decrease the risk that users retain lingering access to systems and therefore will decrease the risk of inaccurate, invalid, and unauthorized transactions being processed by systems that could ultimately impact financial reporting.
6	<b>Finding</b>	Documentation of the periodic review of POA&Ms did not exist. Several instances of known security weaknesses did not correspond to a POA&M.
	<b>Recommendation</b>	Grant Thornton recommends that OPM assign specific individuals with overseeing and monitoring POA&Ms to ensure security weaknesses correspond to a POA&M so that they are addressed in a timely manner.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	The agency is able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.

*Continued: Audit of OPM's Fiscal Year 2017 Financial Statements*

7	<b><i>Finding</i></b>	OPM did not have a system in place to identify and generate a complete and accurate listing of users with significant information systems responsibilities.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM establish a means of developing a complete and accurate listing of users with Significant Information System Responsibilities that are required to complete role-based training.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	A comprehensive review of personnel with access to the in-scope applications /systems will decrease the risk that inappropriate individuals maintain access allowing them to perform incompatible functions or functions associated with elevated privileges.
8	<b><i>Finding</i></b>	Entity level policies and procedures are outdated and / or incomplete.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM continue to follow its project management plan to review and approve newly prepared policies so that the policies can be disseminated to stakeholders.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Policies will reflect current operational environment, which will allow personnel to develop and adhere to authorized processes and related controls.
9	<b><i>Finding</i></b>	OPM did not comply with their policies regarding periodic recertification of the appropriateness of user access.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM perform a comprehensive periodic review of the appropriateness of personnel with access to systems.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Two factor authentication will decrease the risk of unauthorized access into OPM systems.

*Continued: Audit of OPM's Fiscal Year 2017 Financial Statements*

10	<b>Finding</b>	Users are not appropriately provisioned and de-provisioned access from OPM's information systems and the data center. OPM did not comply with its policies regarding periodic recertification of the appropriateness of user access.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement physical security access reviews to ensure access to the data center is limited to personnel that require access based on their job responsibilities.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Reviews will limit physical security access.
11	<b>Finding</b>	All six of the financial applications assessed were not compliant with OMB-M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors or Personal Identity Verification (PIV) and OPM policy which requires the two-factor authentication.
	<b>Recommendation</b>	Grant Thornton recommends that OPM implement two-factor authentication for applications.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Two factor authentication will decrease the risk of unauthorized access into OPM systems.
12	<b>Finding</b>	OPM could not provide a system generated listing of all users who have access to systems. System roles and associated responsibilities or functions, including the identification of incompatible role assignments were not documented.
	<b>Recommendation</b>	Grant Thornton recommends that OPM document access rights to systems to include roles, role descriptions, and privileges or activities associated with each role or activity assignments that may cause a segregation of duties conflict.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	A comprehensive understanding of user access rights will decrease the risk that users perform incompatible duties or have access to privileges or roles outside of what is needed to perform their day-to-day duties.

*Continued: Audit of OPM's Fiscal Year 2017 Financial Statements*

13	<b><i>Finding</i></b>	Users are not appropriately provisioned and de-provisioned access from OPM's information systems and the data center. OPM did not comply with their policies regarding periodic recertification of the appropriateness of user access.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM ensure policies and procedures governing the provisioning and de-provisioning of access to information systems are followed in a timely manner and documentation of completion of these processes is maintained.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Policies will reflect current operational environment, which will allow personnel to develop and adhere to authorized processes and related controls.
14	<b><i>Finding</i></b>	Security events were not reviewed in a timely manner.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM review audit logs on a pre-defined periodic basis for violations or suspicious activity and identify individuals responsible for follow up or elevation of issues to the appropriate team members for review. The review of audit logs should be documented for record retention purposes.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	A thorough review of audit logs decreases the risk that suspicious activity that occurs may go undetected and therefore may not be addressed in a timely manner.
15	<b><i>Finding</i></b>	OPM could not provide a system generated listing of all users who have access to systems. System roles and associated responsibilities or functions, including the identification of incompatible role assignments were not documented.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM establish a means of documenting all users who have access to system.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	A comprehensive understanding of user access rights will decrease the risk that users perform incompatible duties or have access to privileges or roles outside of what is needed to perform their day-to-day duties.



*Continued: Audit of OPM's Fiscal Year 2017 Financial Statements*

16	<b><i>Finding</i></b>	OPM has not developed comprehensive configuration management policies and procedures governing changes that is formally approved and disseminated to OPM personnel. One instance of patches were not applied in a timely manner.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM establish a comprehensive configuration management plan that includes roles and responsibilities and outlines details supporting authorization, testing and documentation requirements.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Decreases the risk that unauthorized or erroneous changes to the mainframe configuration may be introduced without detection by system owners.
17	<b><i>Finding</i></b>	OPM did not have the ability to generate a complete and accurate listing of modifications made to configuration items to systems.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM establish a methodology to systematically track all configuration items that are migrated to production and be able to produce a complete and accurate listing of all configuration items for both internal and external audit purposes, which will in turn support closer monitoring and management of the configuration management process.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Decreases the risk that unauthorized or erroneous changes to the mainframe and midrange environments configuration may be introduced without detection by system owners.
18	<b><i>Finding</i></b>	OPM did not maintain a security configuration checklist for platforms.
	<b><i>Recommendation</i></b>	Grant Thornton recommends that OPM enforce existing policy developed by OPM, vendors or federal agencies requiring mandatory security configuration settings and implement a process to periodically validate that the settings are appropriate.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30 2018, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Restrictive security settings in place for components and a periodic assessment to ensure that such settings are in place and appropriate decreases the risk that the confidentiality, integrity, and / or availability of financial data is compromised.



**Title: Audit of OPM's Travel Card Program**

**Report #: 4A-CF-00-15-049**

**Date: January 16, 2018**

<b>Rec. #</b>		
1	<b>Finding</b>	Travel Operations lacks clear, concise, and accurate policies and procedures, governing their Travel Charge Card Program.
	<b>Recommendation</b>	The OIG recommends that Travel Operations ensure that all travel card policies and procedures, governing OPM's travel card program, are accurate and consistent with one another and contain all areas/ requirements outlined by laws and regulations pertaining to OPM's government travel card program.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Current, clear, and accurate policies and procedures will help to reduce the potential for fraud, waste, and abuse of the travel card program.
2	<b>Finding</b>	See #1 for description.
	<b>Recommendation</b>	The OIG recommends that Travel Operations ensure that roles and responsibilities are clearly articulated to avoid ambiguity of delegated duties.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Consistency creates less confusion among users and increases the accountability between employees and their program managers.
3	<b>Finding</b>	See #1 for description.
	<b>Recommendation</b>	The OIG recommends that Travel Operations collaborate with OPM's Employee Services to formulate written penalties to deter misuse of OPM's travel charge cards.
	<b>Status</b>	The agency partially agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Current, clear, and accurate policies and procedures will help to reduce the potential for fraud, waste, and abuse of the travel card program.

*Continued: Audit of OPM's Travel Card Program*

4	<b><i>Finding</i></b>	See #1 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations immediately replace the Charge Card Management Plan, dated May 5, 2006, located on THEO, with the version dated January 2017. Travel Operations should also ensure that THEO is immediately updated when a new version of the Charge Card Management Plan is released or updated.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Current, clear, and accurate policies and procedures will help to reduce the potential for fraud, waste, and abuse of the travel card program.
5	<b><i>Finding</i></b>	Out of 75 travel card program participants sampled, we determined that 93 percent of the participants had not completed the required training.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations ensure all travel cardholders, approving officials, the agency program coordinator, and agency organizational program coordinators, that have not taken the mandatory initial and refresher training, complete the training within an appropriate timeframe, or suspend the use of their travel card and/or oversight duties until training is completed.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Properly trained participants can lead to the decrease in card misuse and abuse.
6	<b><i>Finding</i></b>	See #5 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations formally appoint approving officials and program coordinators through appointment letters, which outline their basic responsibilities and duties related to the travel card operations for their respective program office.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Participants that are properly informed of their responsibilities can lead to the decrease in card misuse and abuse.

*Continued: Audit of OPM's Travel Card Program*

7	<b>Finding</b>	See #5 for description.
	<b>Recommendation</b>	The OIG recommends that Travel Operations coordinate and partner with OPM program approving officials, program coordinators, and any appropriate program offices to implement controls to ensure card users and oversight personnel receive the required training on the appropriate use, controls and consequences of abuse before they are given a card, and/or appointment to the position. Documentation should be maintained to support the completion of initial and refresher training.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Properly trained participants can lead to the decrease in card misuse and abuse.
8	<b>Finding</b>	Out of the 324 travel card transactions selected for testing, we found that 33 transactions, totaling \$8,158, were missing travel authorizations and 28 transactions, totaling \$27,627, were missing required receipts.
	<b>Recommendation</b>	The OIG recommends that Travel Operations strengthen its oversight and monitoring of travel card transactions, to include but not be limited to, ensuring travel cards are being used and approved in accordance with regulations and guidance.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Supported transactions decrease the risk for abuse or misuse of the travel card and agency resources.
9	<b>Finding</b>	See #8 for description.
	<b>Recommendation</b>	The OIG recommends that Travel Operations provide frequent reminders to the approving officials on their responsibilities when reviewing travel authorizations and vouchers. Reminders should include such things as GSA's best practices for travel charge cards to ensure travel cardholders submit receipts for expenses over \$75 when submitting their vouchers, and that travel authorizations are approved prior to travel.
	<b>Status</b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Supported transactions decrease the risk for abuse or misuse of the travel card and agency resources.

*Continued: Audit of OPM's Travel Card Program*

10	<b><i>Finding</i></b>	See #8 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations develop written procedures for their Compliance Review and Voucher Review processes. At a minimum, procedures should include verifying and validating travel authorizations, receipts, and vouchers.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Current, clear, and accurate policies and procedures will help to reduce the potential for fraud, waste, and abuse of the travel card program.
11	<b><i>Finding</i></b>	We determined that 21 restricted cardholders made 68 cash advance transactions that exceeded their seven-day limit, totaling \$17,493. Three of the 21 restricted cardholders also exceeded their billing cycle limits, totaling \$3,509.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations ensure organizational program coordinators review and certify monthly ATM Reports to help identify cardholder cash advances taken in excess of their ATM limit.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	A robust system of internal controls over the ATM cash advance decreases the risk that cash advances are used for expenses unrelated to Government travel.
12	<b><i>Finding</i></b>	See #11 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations follow up with organizational program coordinators to ensure that appropriate actions are taken against employees who have used their travel card for unauthorized transactions during each billing cycle.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	A robust system of internal controls over the ATM cash advance decreases the risk that cash advances are used for expenses unrelated to Government travel.

*Continued: Audit of OPM's Travel Card Program*

13	<b><i>Finding</i></b>	Travel Operations did not provide support that cardholder accounts with delinquencies of 61 days or more were suspended or cancelled.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations ensure that payments are made or to obtain a remediation plan for all outstanding balances on delinquent accounts, totaling \$61,189.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Removing cards in the hands of a delinquent cardholder decreases the chances for fraud, misuse, and abuse of the travel card.
14	<b><i>Finding</i></b>	See #13 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations strengthen internal controls to confirm that delinquent accounts are monitored and ensure that all delinquent cardholder accounts are either suspended or canceled, as appropriate.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Removing cards in the hands of a delinquent cardholder decreases the chances for fraud, misuse, and abuse of the travel card.
15	<b><i>Finding</i></b>	Travel Operations did not immediately cancel 176 travel card accounts of employees that separated from OPM.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations ensure that an analysis is routinely performed to certify that travel cards are not used after the separation date.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Cancelling cards immediately upon termination of employment decreases the opportunity for continued use, which can result in travel card misuse and abuse.

*Continued: Audit of OPM's Travel Card Program*

16	<b><i>Finding</i></b>	See #15 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations implement stronger internal controls to ensure that travel card accounts are immediately cancelled upon separation of the cardholder's employment.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Cancelling cards immediately upon termination of employment decreases the opportunity for continued use, which can result in travel card misuse and abuse.
17	<b><i>Finding</i></b>	We were unable to determine if inactive cardholder's accounts had been deactivated because documentation was not provided to show that periodic reviews of cardholder activity had been completed.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations identify cardholders that have not used their travel card for one year or more and deactivate travel cards in a timely manner.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.
18	<b><i>Finding</i></b>	See #17 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations enforce policies and procedures to conduct periodic reviews of travel card accounts to ensure cards are needed by the employees to which they are issued.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.
19	<b><i>Finding</i></b>	See #17 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations establish and implement controls to properly document and retain support for the periodic reviews of inactivity.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.

*Continued: Audit of OPM's Travel Card Program*

20	<b><i>Finding</i></b>	Travel Operations does not have controls in place to ensure that the travel card data reported in the Annual Financial Report is accurate.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations provide support to validate the travel card information provided in Table 18. Furthermore, we recommend Travel Operations improve internal controls over its travel card reporting process to ensure the integrity of the travel card data reported in the AFR. These controls should include verification and validation of the travel card information prior to reporting it in the AFR.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Validating the travel card data ensures the AFR information is not erroneous.
21	<b><i>Finding</i></b>	See #20 for description.
	<b><i>Recommendation</i></b>	The OIG recommends that Travel Operations properly cite the source of the travel card data reported in OPM's AFR when the data is provided from sources external to OPM.
	<b><i>Status</i></b>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to resolve the finding; however, we are still reviewing it as part of our current risk assessment.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Properly citing the source of the data provides transparency to readers.

**Title: OPM's Award of a Credit Monitoring and Identity Theft Services Contract to ID Experts**

**Report #: 4A-OO-00-17-035**

**Date: February 28, 2018**

<b>Rec. #</b>		
1	<b>Finding</b>	OPO did not comply with the FAR requirements and OPM's policies and procedures in awarding the ID Experts contract.
	<b>Recommendation</b>	The OIG recommends that OPO immediately update its policies and procedures, to include but not be limited to, guidance for contract document approvals, emergency acquisitions, and contract file completion to ensure compliance with the FAR. When completed, contracting staff should be notified of the changes.
	<b>Status</b>	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If effective policies and procedures are in place then it will help ensure contracting officers are safeguarding the interests of the United States in its contractual relationship.
2	<b>Finding</b>	OPO needs to strengthen its review controls over the procurement process.
	<b>Recommendation</b>	The OIG recommends that OPO implement controls to ensure that each contract complies with the FAR requirements and internal policies and procedures. This includes, but is not limited to, documenting and approving all contracting actions prior to contract award, as required by the "Review & Approval Levels" and "Contracting Policy 1.102(s), Contract Review Board."
	<b>Status</b>	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and submitted evidence to the OIG for closure review.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If effective controls are in place to ensure the contract is in compliance, it will increase the likelihood that OPM is obtaining a qualified vendor.

**Title: Audit of OPM's Common Services**

**Report #: 4A-CF-00-16-055**

**Date: March 29, 2018**

<b>Rec. #</b>		
1	<b>Finding</b>	Data Entry Errors were identified in the common services distribution calculation.
	<b>Recommendation</b>	The OIG recommends that the OCFO implement a process to correct identified errors in the same fiscal year.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If effective controls are in place to ensure errors are identified, funding sources will not be incorrectly charged for their share of common services.



*Continued: Audit of OPM's Common Services*

2	<b>Finding</b>	See #1 for description
	<b>Recommendation</b>	The OIG recommends that the OCFO strengthen its internal controls to ensure that the distribution basis figures are properly supported, reviewed, and approved prior to billing the funding sources.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that corrective actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	If effective controls are in place to ensure errors are identified, funding sources will not be incorrectly charged for their share of common services.
3	<b>Finding</b>	The OCFO could not produce documentation to support (1) that the Director approved the fiscal year 2017 common services cost of \$105,101,530; (2) a change in Human Resources Solutions' common services January billing; and (3) how it determined the amount charged to the Office of the Inspector General.
	<b>Recommendation</b>	The OIG recommends that the OCFO provide documentation to support the Director's approval of the common services cost.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that corrective actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Maintaining supporting documentation supports the common services cost and billing charges which help to ensure that OPM's funding sources have not been mischarged for common services.
4	<b>Finding</b>	See #3 for description.
	<b>Recommendation</b>	The OIG recommends that the OCFO maintain proper documentation to support all common services data, to include but not be limited to verbal agreements, calculations, methodology, distribution, and billing, to ensure completeness and transparency.
	<b>Status</b>	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Maintaining supporting documentation supports the common services cost and billing charges which help to ensure that OPM's funding sources have not been mischarged for common services.

*Continued: Audit of OPM's Common Services*

5	<b><i>Finding</i></b>	The OCFO's fiscal year 2017 common services bill did not identify the "Unallocated" amount, which is set aside for emergency purposes.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCFO reformat its budget levels to ensure all costs are appropriately itemized and/or contain full disclosure of all costs, to ensure transparency.
	<b><i>Status</i></b>	The agency did not agree with the recommendation. Evidence to support their disagreement has not yet been provided.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	By providing transparent budget levels, senior official will be aware of all the services that they are being charged for.

## II. INFORMATION SYSTEMS AUDITS

This section describes the open recommendations from audits of the information systems operated by OPM, FEHBP insurance carriers, and OPM contractors.

<b>Title:</b> Federal Information Security Management Act Audit FY 2008 <b>Report #:</b> 4A-CI-00-08-022 <b>Date:</b> September 23, 2008		
Rec. #		
1	<b>Finding</b>	<u>Security Controls Testing</u> – The Federal Information Security Management Act (FISMA) requires agencies to test the security controls of all of their systems on an annual basis. However, we determined that the security controls were not tested for three of OPM’s systems in FY 2008.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
2	<b>Finding</b>	<u>Contingency Plan Testing</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. We determined that the contingency plans for four OPM systems were not adequately tested in FY 2008.
	<b>Recommendation</b>	The OIG recommends that OPM’s program offices test the contingency plans for each system on an annual basis.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

<b>Title:</b> Federal Information Security Management Act Audit FY 2009 <b>Report #:</b> 4A-CI-00-09-031 <b>Date:</b> November 5, 2009		
Rec. #		
6	<b>Finding</b>	<u>Security Controls Testing:</u> FISMA requires agencies to test the security controls of their systems on an annual basis. In FY 2009, two systems did not have adequate security control tests.
	<b>Recommendation</b>	The OIG recommends OPM ensure that an annual test of security controls has been completed for all systems. The IT security controls should be immediately tested for the two systems that were not subject to testing in FY 2009.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

*Continued: Federal Information Security Management Act Audit FY 2009*

9	<b>Finding</b>	<u>Contingency Plan Testing</u> : FISMA requires agencies to test the contingency plans of their systems on an annual basis. In FY 2009, 11 systems did not have adequate contingency plan tests.
	<b>Recommendation</b>	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 11 systems that were not subject to testing in FY 2009.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

**Title: Federal Information Security Management Act Audit FY 2010**

**Report #: 4A-CI-00-10-019**

**Date: November 10, 2010**

<b>Rec. #</b>		
10	<b>Finding</b>	<u>Test of Security Controls</u> : FISMA requires agencies to test the security controls of their systems on an annual basis. In FY 2010, 15 systems did not have adequate security control tests.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
30	<b>Finding</b>	<u>Contingency Plan Testing</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2010, 13 systems were not subject to adequate contingency plan tests.
	<b>Recommendation</b>	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 13 systems that were not subject to adequate testing in FY 2010.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

**Title: Federal Information Security Management Act Audit FY 2011**  
**Report #: 4A-CI-00-11-009**  
**Date: November 9, 2011**

<b>Rec. #</b>		
6	<b>Finding</b>	<u>Risk Management</u> : NIST SP 800-39 states that agencies should establish and implement "Governance structures [that] provide oversight for the risk management activities." The OCIO does not currently have a formal methodology for managing risk at an organization-wide level.
	<b>Recommendation</b>	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.
7	<b>Finding</b>	<u>Test of Security Controls</u> : FISMA requires agencies to test the security controls of their systems on an annual basis. In FY 2011, 12 systems were not subject to adequate security control tests.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
19	<b>Finding</b>	<u>Contingency Plan Testing</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2011, eight systems were not subject to adequate contingency plan tests.
	<b>Recommendation</b>	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the eight systems that were not subject to adequate testing in FY 2011.
	<b>Status</b>	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

**Title: Federal Information Security Management Act Audit FY 2012**  
**Report #: 4A-CI-00-12-016**  
**Date: November 5, 2011**

<b>Rec. #</b>		
2	<b>Finding</b>	<u>Risk Management</u> : NIST SP 800-39 states that agencies should establish and implement “Governance structures [that] provide oversight for the risk management activities.” The OCIO does not currently have a formal methodology for managing risk at an organization-wide level.
	<b>Recommendation</b>	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive Function.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.
11	<b>Finding</b>	<u>Multi-factor Authentication</u> : OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by the beginning of FY 2012. However, as of the end of FY 2012, none of the 47 major systems at OPM require PIV authentication.
	<b>Recommendation</b>	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for authenticating to information systems.
14	<b>Finding</b>	<u>Test of Security Controls</u> : FISMA requires agencies to test the security controls of its systems on an annual basis. In FY 2012, 13 systems were not subject to adequate security control tests.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b>Status</b>	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

*Continued: Federal Information Security Management Act Audit FY 2012*

15	<b>Finding</b>	<u>Contingency Plan Testing</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2012, eight systems were not subject to adequate contingency plan tests.
	<b>Recommendation</b>	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the eight systems that were not subject to adequate testing in FY 2012.
	<b>Status</b>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

**Title: Federal Information Security Management Act Audit FY 2013**  
**Report #: 4A-CI-00-13-021**  
**Date: November 21, 2013**

<b>Rec. #</b>		
2	<b>Finding</b>	<u>SDLC Methodology</u> : OPM has a history of troubled system development projects. In our opinion, the root cause of these issues relates to the lack of central policy and oversight of systems development.
	<b>Recommendation</b>	The OIG recommends that the OCIO develop a plan and timeline to enforce the new SDLC policy to all of OPM's system development projects.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring stability of systems development projects.
3	<b>Finding</b>	<u>Agency-wide Risk Management</u> : the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2013, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were not all fully implemented.
	<b>Recommendation</b>	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.

*Continued: Federal Information Security Management Act Audit FY 2013*

11	<b><i>Finding</i></b>	<u>Multi-factor Authentication</u> : OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by the beginning of FY 2012. However, as of the end of the FY 2013, none of the 47 major systems at OPM require PIV authentication.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for authenticating to information systems.
13	<b><i>Finding</i></b>	<u>Test of Security Controls</u> : FISMA requires agencies to test the security controls of its systems on an annual basis. In FY 2013, 13 systems were not subject to adequate security control tests.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b><i>Status</i></b>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
14	<b><i>Finding</i></b>	<u>Contingency Plan Testing</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2013, seven were not subject to adequate contingency plan tests.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be tested for the systems that were not subject to adequate testing in FY 2013 as soon as possible.
	<b><i>Status</i></b>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for recovering from an unplanned system outage.



**Title: Audit of IT Security Controls – OPM’s DTP**  
**Report #: 4A-CI-00-14-015**  
**Date: June 6, 2014**

<b>Rec. #</b>		
4	<b>Finding</b>	<u>Configuration Change Control</u> : DTP application programmers have the technical ability to develop a change and move it into production without following the appropriate change control process.
	<b>Recommendation</b>	The OIG recommends that the OCIO make the appropriate system modifications to ensure appropriate segregation of duties are enforced within DTP.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing changes to information systems.
5	<b>Finding</b>	<u>Configuration Change Control</u> : DTP application programmers have the technical ability to develop a change and move it into production without following the appropriate change control process.
	<b>Recommendation</b>	The OIG recommends that the OCIO make the appropriate organizational modification to ensure a business unit independent of the application developers migrates changes into production. That same business unit should be responsible for validating that all elements of the SDLC were followed, changes were appropriately tested, and all documentation is valid and approved prior to migrating changes into production.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing changes to information systems.

**Title: Federal Information Security Management Act Audit FY 2014**  
**Report #: 4A-CI-00-14-016**  
**Date: November 12, 2014**

<b>Rec. #</b>		
2	<b>Finding</b>	<u>SDLC Methodology</u> : OPM has a history of troubled system development projects. In our opinion, the root cause of these issues relates to the lack of central policy and oversight of systems development.
	<b>Recommendation</b>	The OIG continues to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy to all of OPM’s system development projects.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring stability of systems development projects.

*Continued: Federal Information Security Management Act Audit FY 2014*

3	<b>Finding</b>	<u>Security Assessment and Authorization</u> : Eleven OPM systems are operating without an active Security Assessment and Authorization.
	<b>Recommendation</b>	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
4	<b>Finding</b>	<u>Security Assessment and Authorization</u> : Several OPM systems are operating without an active Security Assessment and Authorization. In our opinion, one root cause of this issue relates to the lack of accountability for system owners that fail to subject their systems to the Authorization process.
	<b>Recommendation</b>	The OIG recommends that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
6	<b>Finding</b>	<u>Agency-wide Risk Management</u> : the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were not all fully implemented.
	<b>Recommendation</b>	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.

*Continued: Federal Information Security Management Act Audit FY 2014*

7	<b>Finding</b>	<u>Baseline Configurations</u> : In FY 2014, OPM has continued its efforts toward formalizing baseline configurations for critical applications, servers, and workstations. At the end of the fiscal year, the OCIO had established baselines for several operating systems, but not for all that the agency uses in its environment.
	<b>Recommendation</b>	The OIG recommends that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM including, but not limited to, [REDACTED] and [REDACTED].
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that information systems are initially configured in a secure manner.
8	<b>Finding</b>	<u>Configuration Auditing</u> : There are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.
	<b>Recommendation</b>	The OIG recommends the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 7 has been completed.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that servers are in compliance with approved security settings.
11	<b>Finding</b>	<u>Vulnerability Scanning</u> : We were told in an interview that OPM performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2014.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for detecting and vulnerabilities.

*Continued: Federal Information Security Management Act Audit FY 2014*

12	<b>Finding</b>	<u>Vulnerability Scanning</u> : The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for tracking and remediating vulnerabilities.
14	<b>Finding</b>	<u>Patching Management</u> : Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	<b>Recommendation</b>	The OIG recommends the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for keeping information systems up-to-date with patches and service packs.
21	<b>Finding</b>	<u>Multi-factor Authentication</u> : OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by FY 2012. However, as of the end of the FY 2014, none of the 47 major systems at OPM require PIV authentication.
	<b>Recommendation</b>	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for authenticating to information systems.
23	<b>Finding</b>	<u>Test of Security Controls</u> : FISMA requires agencies to test the security controls of all of their systems on an annual basis. In FY 2014, 10 systems were not subject to adequate security control tests.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b>Status</b>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

*Continued: Federal Information Security Management Act Audit FY 2014*

24	<b><i>Finding</i></b>	<u>Contingency Plans</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. We received updated contingency plans for 41 out of 47 information systems on OPM’s master system inventory.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCIO ensure that all of OPM’s major systems have contingency plans in place and are reviewed and updated annually.
	<b><i>Status</i></b>	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for recovering from an unplanned system outage.
25	<b><i>Finding</i></b>	<u>Contingency Plan Testing</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2014, eight were not subject to adequate contingency plan tests.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM’s program offices test the contingency plans for each system on an annual basis. The contingency plans should be tested for the systems that were not subject to adequate testing in FY 2014 as soon as possible.
	<b><i>Status</i></b>	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for recovering from an unplanned system outage.
28	<b><i>Finding</i></b>	<u>Contractor System Documentation</u> : The OCIO maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, many of the documented ISAs have expired.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.

*Continued: Federal Information Security Management Act Audit FY 2014*

29	<b>Finding</b>	<u>Contractor System Documentation</u> : While the OCIO tracks ISAs, it does not track Memorandums of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. We were told that program offices were responsible for maintaining MOU/As. While we have no issue with the program offices maintaining the memorandums, the OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.

**Title: Flash Audit: OPM's Infrastructure Improvement**

**Report #: 4A-CI-00-15-055**

**Date: June 17, 2015**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Project Management Activities</u> : OPM has not yet defined the scope and budget sources for the entire Infrastructure as a Service (IaaS) Project. The agency has not followed standard, and critical, project management steps, many of which are required by OMB.
	<b>Recommendation</b>	The OIG recommends that OPM's OCIO complete an OMB Major IT Business Case document as part of the FY 2017 budget process and submit this document to OMB for approval. Associated with this effort, the OCIO should complete its assessment of the scope of the migration process, the level of effort required to complete it, and its estimated costs. Furthermore, the OCIO should implement the project management processes required by OMB and recommended by ISACA's COBIT and the COSO framework.
	<b>Status</b>	OPM subsequently agreed to implement this recommendation. The OIG reviewed evidence submitted by OPM to support closure of the recommendation and provided comments explaining why this evidence was not sufficient to close the recommendation. OPM is taking further corrective actions. The OIG has not yet received evidence that full implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for minimizing the risk of a major project failure.

**Title: Audit of Information Security Controls of OPM's AHBOSS**  
**Report #: 4A-RI-00-15-019**  
**Date: July 29, 2015**

<b>Rec. #</b>		
3	<b>Finding</b>	<u>Identification and Authentication (Organizational Users)</u> : General Dynamics Information Technology (GDIT) has not implemented multi-factor authentication utilizing PIV cards for access to AHBOSS, in accordance with OMB Memorandum M-11-11.
	<b>Recommendation</b>	The OIG recommends that RS require GDIT to enforce PIV authentication for all required AHBOSS users.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying and authenticating system users.
4	<b>Finding</b>	<u>Physical Access Control</u> : the data center hosting AHBOSS uses electronic card readers to control access to the building and data center. It has no multi-factor authentication or [REDACTED] controls in place.
	<b>Recommendation</b>	The OIG recommends that RS ensure that the physical access controls at the data center hosting AHBOSS are improved. At a minimum, we expect to see multi-factor authentication at data center entrances and controls.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for physical access the data center.
6	<b>Finding</b>	<u>Vulnerability Scanning: System Patching</u> – Our independent vulnerability scans indicated that critical patches and service packs are not always implemented in a timely manner.
	<b>Recommendation</b>	The OIG recommends that RS require GDIT to implement procedures and controls to ensure that servers and databases are installed with appropriate patches, service packs, and hotfixes on a timely basis.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for maintaining current and up-to-date system software.

*Continued: Audit of Information Security Controls of OPM's AHBOSS*

7	<b>Finding</b>	<u>Configuration Settings</u> : GDIT performs a manual compliance audit of configuration settings on all AHBOSS servers each month. Automated tools would be a more effective and thorough method of compliance auditing than the manual process currently in place.
	<b>Recommendation</b>	The OIG recommends that RS ensure that GDIT utilize automated software tools to perform configuration compliance audits of the AHBOSS servers.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying insecure configuration settings.

**Title: Federal Information Security Management Act Audit FY 2015**  
**Report #: 4A-CI-00-15-011**  
**Date: November 10, 2015**

<b>Rec. #</b>		
2	<b>Finding</b>	<u>SDLC Methodology</u> : OPM has a history of troubled system development projects. In our opinion, the root cause of these issues relates to the lack of central policy and oversight of systems development.
	<b>Recommendation</b>	The OIG continues to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy to all of OPM's system development projects.
	<b>Status</b>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring stability of systems development projects.
3	<b>Finding</b>	<u>Security Assessment and Authorization</u> : Eleven OPM systems are operating without an active Security Assessment and Authorization.
	<b>Recommendation</b>	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.



*Continued: Federal Information Security Management Act Audit FY 2015*

4	<b>Finding</b>	<u>Security Assessment and Authorization</u> : Several OPM systems are operating without an active Security Assessment and Authorization. In our opinion, one root cause of this issue relates to the lack of accountability for system owners that fail to subject their systems to the Authorization process.
	<b>Recommendation</b>	The OIG recommends that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
7	<b>Finding</b>	<u>Test of Security Controls</u> : FISMA requires agencies to test the security controls of all of its systems on an annual basis. In FY 2015, 16 systems were not subject to adequate security control tests.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
8	<b>Finding</b>	<u>Baseline Configurations</u> : In FY 2015, OPM has continued its efforts toward formalizing baseline configurations for critical applications, servers, and workstations. The OCIO had established baselines for several operating systems, but not for all that the agency uses in its environment.
	<b>Recommendation</b>	The OIG recommends that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM including, but not limited to, [REDACTED], and [REDACTED].
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that information systems are initially configured in a secure manner.

*Continued: Federal Information Security Management Act Audit FY 2015*

9	<b>Finding</b>	<u>Configuration Auditing</u> : There are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.
	<b>Recommendation</b>	The OIG recommends the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 7 has been completed.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that servers are in compliance with approved security settings.
10	<b>Finding</b>	<u>Vulnerability Scanning</u> : We were told in an interview that OPM performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2014.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for detecting and remediating vulnerabilities.
11	<b>Finding</b>	<u>Vulnerability Scanning</u> : The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for tracking and remediating vulnerabilities.

*Continued: Federal Information Security Management Act Audit FY 2015*

13	<b>Finding</b>	<u>Unsupported Software</u> : The results of our vulnerability scans indicated that OPM’s production environment contains severely out-of-date and unsupported software and operating platforms.
	<b>Recommendation</b>	The OIG recommends the OCIO implement a process to ensure that only supported software and operating platforms are utilized within the network environment.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring up-to-date software and operating platforms.
14	<b>Finding</b>	<u>Patching Management</u> : Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	<b>Recommendation</b>	The OIG recommends the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for keeping information systems up-to-date with patches and service packs.
16	<b>Finding</b>	<u>Multi-factor Authentication</u> : OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by FY 2012. However, as of the end of the FY 2014, none of the 47 major systems at OPM require PIV authentication.
	<b>Recommendation</b>	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for authenticating to information systems.

*Continued: Federal Information Security Management Act Audit FY 2015*

18	<b>Finding</b>	<u>Agency-wide Risk Management</u> : The OCIO organized a Risk Executive Function comprised of several IT security professionals. However, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were not all fully implemented.
	<b>Recommendation</b>	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.
24	<b>Finding</b>	<u>Contingency Plans</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. We received updated contingency plans for 41 out of 47 information systems on OPM's master system inventory.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that all of OPM's major systems have contingency plans in place and are reviewed and updated annually.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.
25	<b>Finding</b>	<u>Contingency Plan Testing</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2014, eight were not subject to adequate contingency plan tests.
	<b>Recommendation</b>	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis. The contingency plans should be tested for the systems that were not subject to adequate testing in FY 2014 as soon as possible.
	<b>Status</b>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

*Continued: Federal Information Security Management Act Audit FY 2015*

26	<b>Finding</b>	<u>Contractor System Documentation</u> : The OCIO maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, many of the documented ISAs have expired.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.
27	<b>Finding</b>	<u>Contractor System Documentation</u> : While the OCIO tracks ISAs, it does not track Memorandums of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. We were told that program offices were responsible for maintaining MOU/As. While we have no issue with the program offices maintaining the memorandums, the OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.

**Title: Second Status Report: OPM's Infrastructure Improvement**  
**Report #: 4A-CI-00-16-037**  
**Date: May 18, 2016**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Major IT Business Case</u> : OPM completed a Business Case for its infrastructure improvement project. However, OPM officials failed to perform almost all of the capital planning activities that are required to be associated with a Business Case document.
	<b>Recommendation</b>	The OIG recommends that OPM complete an Analysis of Alternatives as described in the Capital Programming Guide supplement to OMB Circular A-11 as soon as possible. This analysis should recognize changes in the internal and external environment and no consideration should be given to funds already spent associated with the Project (i.e., avoid the sunk cost fallacy).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for minimizing the risk of a major project failure.

*Continued: Second Status Report: OPM's Infrastructure Improvement*

2	<b>Finding</b>	<u>Lifecycle Cost Estimates</u> : OPM's Business Case submitted to OMB with the FY 2017 budget request outlines the costs already incurred for this Project along with reasonable short-term cost estimates to finish developing the IaaS portion. However, its cost estimates for modernizing and migrating its information systems to the new environment are unsubstantiated because of the incomplete inventory and technical analysis.
	<b>Recommendation</b>	The OIG recommends that OPM leverage the application profiling scoring framework to develop cost estimates for modernizing and/or migrating all OPM information systems, and use this information to support the capital planning activities referenced in Recommendation 1. The Business Case should be continuously updated to reflect these cost estimates as they become more concrete.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for minimizing the risk of a major project failure.

**Title: Audit of OPM's Web Application Security Review**  
**Report #: 4A-CI-00-16-061**  
**Date: October 13, 2016**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Web Application Inventory</u> : OPM does not maintain an adequate inventory of web applications. OPM's OCIO has developed an inventory of servers, databases, and network devices, but the inventory does not identify the purpose, role, or owner of each device.
	<b>Recommendation</b>	The OIG recommends that OPM create a formal and comprehensive inventory of web applications. The inventory should identify which applications are public facing and contain personally identifiable information or sensitive agency information, identify the application owner, and itemize all system interfaces with the web application.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying and documenting web based applications.

*Continued: Audit of OPM's Web Application Security Review*

2	<b>Finding</b>	<u>Policies and Procedures</u> : OPM maintains information technology (IT) security policies and procedures that address NIST SP 800-53 security controls. OPM also maintains system development policies and standards. While these policies, procedures, and standards apply to all IT assets, they are written at a high level and do not address some critical areas specific to web application security and development.
	<b>Recommendation</b>	The OIG recommends that OPM create or update its policies and procedures to provide guidance specific to the hardening of web server operating systems and the secure design and coding of web-based applications.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for establishing policy and procedures governing the hardening of web applications.
3	<b>Finding</b>	<u>Web Application Vulnerability Scanning</u> : While the OCIO was able to provide historical server vulnerability scan results, we were told that there is not a formal process in place to perform routine credentialed web application vulnerability scans (however, ad-hoc non-credentialed scans were performed).
	<b>Recommendation</b>	The OIG recommends that OPM implement a process to perform credentialed web application vulnerability scans and track any identified vulnerabilities until they are remediated.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for detecting and tracking vulnerabilities.
4	<b>Finding</b>	<u>Web Application Vulnerability Scanning</u> : The results of the credentialed web application scans that we performed during this review indicate that several applications and the servers hosting these applications contain security weaknesses.
	<b>Recommendation</b>	The OIG recommends that OPM analyze our scan results to identify false positives and remediate any verified vulnerabilities.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for remediating vulnerabilities.

**Title: Federal Information Security Management Act Audit FY 2016**  
**Report #: 4A-CI-00-16-039**  
**Date: November 9, 2016**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Security Management Structure</u> : OPM has experienced a high turnover rate for ISSO and CISO positions and has struggled to backfill these vacancies.
	<b>Recommendation</b>	The OIG recommends that OPM hire a sufficient number of ISSOs to adequately support all of the agency's major information systems.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security.
3	<b>Finding</b>	<u>SDLC Methodology</u> : OPM has a history of troubled system development projects. In our opinion, the root cause of these issues relates to the lack of central policy and oversight of systems development.
	<b>Recommendation</b>	The OIG continues to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy on all of OPM's system development projects.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring stability of systems development projects.
4	<b>Finding</b>	<u>Security Assessment and Authorization</u> : OPM systems are operating without an active Security Assessment and Authorization.
	<b>Recommendation</b>	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
5	<b>Finding</b>	<u>Security Assessment and Authorization</u> : Several OPM systems are operating without an active Security Assessment and Authorization. In our opinion, one root cause of this issue relates to the lack of accountability for system owners that fail to subject their systems to the Authorization process.
	<b>Recommendation</b>	The OIG recommends that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.



*Continued: Federal Information Security Management Act Audit FY 2016*

7	<b>Finding</b>	<u>Agency-wide Risk Management</u> : the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were not all fully implemented.
	<b>Recommendation</b>	The OIG recommends that OPM continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.
8	<b>Finding</b>	<u>Adherence to Remediation Deadlines</u> : Of OPM's 46 major information systems, 43 have POA&M items that are greater than 120 days overdue. Further, 85% of open POA&Ms are over 30 days overdue and over 78% are over 120 days overdue.
	<b>Recommendation</b>	The OIG recommends that OPM adhere to remediation dates for its POA&M weaknesses.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing POA&M weakness remediation.
9	<b>Finding</b>	<u>Contractor System Documentation</u> : The OCIO maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, many of the documented ISAs have expired.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.

*Continued: Federal Information Security Management Act Audit FY 2016*

10	<b>Finding</b>	<u>Contractor System Documentation</u> : While the OCIO tracks ISAs, it does not track Memorandums of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. We were told that program offices were responsible for maintaining MOU/As. While we have no issue with the program offices maintaining the memorandums, the OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.
11	<b>Finding</b>	<u>System Inventory</u> : OPM's system inventory lists the devices and software in the environment, but does not describe the specific servers the software resides on or the information systems the devices and software support.
	<b>Recommendation</b>	The OIG recommends that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for oversight, risk management, and securing the agency's information systems.
12	<b>Finding</b>	<u>Baseline Configurations</u> : In FY 2016, OPM has continued its efforts toward formalizing baseline configurations for critical applications, servers, and workstations. The OCIO had established baselines for several operating systems, but not for all that the agency uses in its environment.
	<b>Recommendation</b>	The OIG recommends that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM including, but not limited to, [REDACTED], and [REDACTED].
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that information systems are initially configured in a secure manner.

*Continued: Federal Information Security Management Act Audit FY 2016*

13	<b><i>Finding</i></b>	<u>Document Deviations to the Standard Configuration Baseline:</u> OPM does not maintain a record of the specific deviations from generic configuration standards.
	<b><i>Recommendation</i></b>	Where an OPM configuration standard is based on a pre-existing generic standard, The OIG recommends that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for effectively auditing a system's actual settings.
14	<b><i>Finding</i></b>	<u>Vulnerability Scanning:</u> We were told in an interview that OPM performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2016.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for detecting and remediating vulnerabilities.
15	<b><i>Finding</i></b>	<u>Unsupported Software:</u> The results of our vulnerability scans indicated that OPM's production environment contains severely out-of-date and unsupported software and operating platforms.
	<b><i>Recommendation</i></b>	The OIG recommends the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for ensuring up-to-date software and operating platforms.

*Continued: Federal Information Security Management Act Audit FY 2016*

16	<b><i>Finding</i></b>	<u>Configuration Auditing</u> : There are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.
	<b><i>Recommendation</i></b>	The OIG recommends the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 13 has been completed.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for ensuring that servers are in compliance with approved security settings.
17	<b><i>Finding</i></b>	<u>Vulnerability Scanning</u> : The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for tracking and remediating vulnerabilities.
18	<b><i>Finding</i></b>	<u>Patching Management</u> : Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	<b><i>Recommendation</i></b>	The OIG recommends the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for keeping information systems up-to-date with patches and service packs.

*Continued: Federal Information Security Management Act Audit FY 2016*

19	<b><i>Finding</i></b>	<u>Contractor Access Termination</u> : OPM does not maintain a complete list of the contractors with access to OPM’s network and the termination process for contractors is de-centralized.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCIO maintain a centralized list of all contractors that have access to the OPM network and use this list to routinely audit all user accounts for appropriateness.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for managing appropriate access to information systems.
20	<b><i>Finding</i></b>	<u>Multi-factor Authentication</u> : OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by FY 2012. However, as of the end of the FY 2016, none of the 46 major systems at OPM require PIV authentication.
	<b><i>Recommendation</i></b>	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for authenticating to information systems.
23	<b><i>Finding</i></b>	<u>Test of Security Controls</u> : FISMA requires agencies to test the security controls of its systems on an annual basis. In FY 2017, 16 systems were not subject to adequate security control tests.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

*Continued: Federal Information Security Management Act Audit FY 2016*

25	<b>Finding</b>	<u>Contingency Plans</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. We received updated contingency plans for 41 out of 47 information systems on OPM's master system inventory.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that all of OPM's major systems have contingency plans in place and are reviewed and updated annually.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.
26	<b>Finding</b>	<u>Contingency Plan Testing</u> : FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis.
	<b>Recommendation</b>	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis.
	<b>Status</b>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

**Title: Audit of Information Security Controls of OPM's FACES**

**Report #: 4A-RS-00-16-035**

**Date: November 21, 2016**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Security Assessment and Authorization</u> : 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.
	<b>Recommendation</b>	The OIG recommends that OPM complete a current Security Assessment and Authorization for FACES.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that risk has been assessed before being approved to operate.

*Continued: Audit of Information Security Controls of OPM's FACES*

2	<b>Finding</b>	<u>System Security Plan (SSP)</u> : The most recent SSP for FACES does not include controls that were added to the current revision of NIST SP 800-53 (Revision 4).
	<b>Recommendation</b>	The OIG recommends that OPM update the FACES SSP in accordance with the agency's policies and NIST standards.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that system security controls are properly documented.
3	<b>Finding</b>	<u>Security Controls Continuous Monitoring</u> : The documentation for 2014 and 2015 indicates that the FACES system was not subject to adequate security control testing in those years. Furthermore, there have not been any security control tests completed for FACES since April 2015.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that the FACES security controls are continuously monitored in accordance with the agency's policy.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
6	<b>Finding</b>	<u>Plan of Action and Milestones Process</u> : Many of the security weaknesses discovered during continuous monitoring activities for FACES were not added to the system's POA&M.
	<b>Recommendation</b>	The OIG recommends that OPM add a POA&M entry for all known weaknesses of FACES.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for addressing weaknesses in a timely manner and limiting system exposure to malicious attacks.
7	<b>Finding</b>	<u>Action plan for Overdue POA&amp;M Items</u> : 20 of the 25 items on the FACES POA&M were over 200 days overdue.
	<b>Recommendation</b>	The OIG recommends that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for addressing weaknesses in an appropriate timeframe and limiting system exposure to malicious attacks.

*Continued: Audit of Information Security Controls of OPM's FACES*

8	<b>Finding</b>	<u>Routinely Review FACES Website</u> : Sensitive personally identifiable information was found to be available on the public facing portion of the FACES website.
	<b>Recommendation</b>	The OIG recommends that OPM implement a process to routinely review the FACES website to ensure that sensitive information is not publically available.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for protecting personally identifiable information maintained by the system.
9	<b>Finding</b>	<u>FACES System's Interconnection Characteristics</u> : FACES is directly connected to at least two of OPM's other major information systems. These interconnections are not documented in the FACES SSP.
	<b>Recommendation</b>	The OIG recommends 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.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for documenting security requirements associated with system interconnections.
10	<b>Finding</b>	<u>Authentication Standards for FACES Servers</u> : The operating system authentication settings for several of the [REDACTED] servers supporting the application did not comply with OPM authentication requirements.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that all FACES servers comply with OPM authentication standards.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for preventing brute force password attacks that could compromise the system and associated accounts.
11	<b>Finding</b>	[REDACTED]
	<b>Recommendation</b>	[REDACTED]
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for adequately segregating the public facing and internal components of FACES.



*Continued: Audit of Information Security Controls of OPM's FACES*

12	<b>Finding</b>	[REDACTED]
	<b>Recommendation</b>	[REDACTED]
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for the protection of sensitive information from inappropriate disclosure.

**Title: Audit of OPM's Security Assessment and Authorization**

**Report #: 4A-CI-00-17-014**

**Date: June 20, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>System Security Plan</u> : The LAN/WAN SSP does not fully and accurately identify all of the security controls applicable to this system.
	<b>Recommendation</b>	The OIG recommends that the OCIO complete an SSP for the LAN/WAN that includes all of the required elements from OPM's SSP template and relevant NIST guidance. This includes, but is not limited to, the specific deficiencies outlined in the section above.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that system security controls are properly documented.
2	<b>Finding</b>	<u>System Controls Assessment</u> : The LAN/WAN security controls assessment likely did not identify vulnerabilities that could have been detected with a thorough test.
	<b>Recommendation</b>	The OIG recommends that the OCIO perform a thorough security controls assessment on the LAN/WAN. This assessment should address the deficiencies listed in the section above, and should be completed after a current and thorough SSP is in place (see Recommendation 1).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

*Continued: Audit of OPM's Security Assessment and Authorization*

3	<b>Finding</b>	<u>Plan of Action and Milestones</u> : OPM was unable to provide a POA&M for the LAN/WAN.
	<b>Recommendation</b>	The OIG recommends that the OCIO update and maintain a complete POA&M list for the LAN/WAN.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for tracking know information security weaknesses.
4	<b>Finding</b>	<u>Other Authorization Packages</u> : Many of the Authorization packages completed as part of the Sprint were not complete.
	<b>Recommendation</b>	The OIG recommends that the OCIO perform a gap analysis to determine what critical elements are missing and/or incomplete for all Authorization packages developed during the Sprint. For systems that reside on the LAN/WAN general support system, the OCIO should also evaluate the impact that an updated LAN/WAN SSP has on these systems' security controls.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that system risk has been assessed before being approved to operate.

**Title: Audit of OPM's Consolidated Business Information System**

**Report #: 4A-CF-00-17-043**

**Date: September 29, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>System Security Plan</u> : The CBIS SSP does not contain all information required by NIST.
	<b>Recommendation</b>	The OIG recommends that OPM update the CBIS SSP in accordance with the agency's policies and NIST standards.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that system security controls are properly documented.

*Continued: Audit of OPM's Consolidated Business Information System*

2	<b>Finding</b>	<u>Incomplete Testing</u> : Three elements of the CBIS security control testing process were missing and/or incomplete.
	<b>Recommendation</b>	The OIG recommends that OPM test the CBIS security controls that were not assessed during the Authorization process.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
3	<b>Finding</b>	<u>Risk Assessment</u> : 29 of the 89 unsatisfied controls were not incorporated into the CBIS risk assessment.
	<b>Recommendation</b>	The OIG recommends that OPM perform an analysis to assess the risk of the 29 control deficiencies that were omitted from the CBIS risk assessment. OPM should update the CBIS risk assessment and POA&Ms to include all identified weaknesses and their risk levels.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks.
6	<b>Finding</b>	<u>Overdue Plan of Action and Milestones</u> : 39 have scheduled completion dates that are more than 6 months overdue.
	<b>Recommendation</b>	The OIG recommends that OPM develop a detailed action plan to remediate all overdue POA&M items and close any that are no longer applicable. This action plan should include realistic estimated completion dates.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for maintaining and documenting POA&M's.
7	<b>Finding</b>	<u>Information System Monitoring</u> : NIST SP 800-53, Revision 4, control SI-4, Information System Monitoring, is not in place for the system.
	<b>Recommendation</b>	The OIG recommends that OPM implement tools and procedures to monitor CBIS according to NIST guidance.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for monitoring information system activity.

**Title: Audit of OPM's Federal Financial System**  
**Report #: 4A-CF-00-17-044**  
**Date: September 29, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Privacy Impact Assessment (PIA)</u> : The Privacy Threshold Analysis and the Privacy Impact Assessment are both incomplete and have not been approved or signed.
	<b>Recommendation</b>	The OIG recommends that OPM fully completes and approves a PIA for BFMS.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying privacy vulnerabilities existing on the information system.
2	<b>Finding</b>	<u>System Security Plan</u> : Outdated, missing, and incomplete information was identified in the SSP.
	<b>Recommendation</b>	The OIG recommends that OPM update the BFMS SSP in accordance with the agency's policies and NIST standards.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that system security controls are properly documented.
3	<b>Finding</b>	<u>Security Assessment Plan and Report</u> : All known security weaknesses were not evaluated during the risk assessment.
	<b>Recommendation</b>	The OIG recommends that OPM perform an analysis to assess the risk of the 38 control deficiencies that were omitted from the risk assessment, and update the BFMS risk assessment and POA&Ms to include all identified weaknesses and their risk levels.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for proper prioritization of weaknesses for remediation.
4	<b>Finding</b>	<u>Continuous Monitoring</u> : There were significant issues with the security control testing process for BFMS.
	<b>Recommendation</b>	The OIG recommends that OPM test the security controls of BFMS in accordance with the ISCMP testing schedule and ensure the results are properly documented.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

*Continued: Audit of OPM's Federal Financial System*

5	<b><i>Finding</i></b>	<u>Contingency Planning</u> : The BFMS contingency plan is not complete.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM update the BFMS contingency plan to include all required information from OPM's template.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for recovering from an unplanned system outage.
6	<b><i>Finding</i></b>	<u>Incomplete Plan of Action and Milestones Lists</u> : The BFMS POA&Ms in the Authorization package do not adhere to OPM's POA&M template or include all of the required information.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM update the BFMS POA&M to include all identified weaknesses and required information per OPM policy.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for tracking know information security weaknesses.
7	<b><i>Finding</i></b>	<u>Overdue Plan of Action and Milestones</u> : A large number of POA&Ms are significantly overdue without revised and approved remediation plans.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for addressing weaknesses in an appropriate timeframe and limiting system exposure to malicious attacks.
8	<b><i>Finding</i></b>	<u>Configuration Settings</u> : Configuration settings are not defined and documented to BFMS.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM document the approved security configuration settings for BFMS.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for ensuring that information systems are initially configured in a secure manner.

*Continued: Audit of OPM's Federal Financial System*

9	<b>Finding</b>	<u>Flaw Remediation:</u> OPM has not had a support contract in place for FFS since 2002.
	<b>Recommendation</b>	The OIG recommends that OPM develop and implement a plan to replace FFS with a fully supported financial system.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring up-to-date software and operating platforms.

**Title: Audit of OPM's SharePoint Implementation**

**Report #: 4A-CI-00-17-030**

**Date: September 29, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>System Classification:</u> OPM has not assessed whether SharePoint should be considered a "major" information system requiring a formal authorization. Additionally, SharePoint is not currently listed on any OPM system inventory.
	<b>Recommendation</b>	The OIG recommends that OPM conduct an analysis to determine the appropriate classification of SharePoint as an information system. If it is classified as a major system, OPM should conduct a full Authorization of SharePoint. If it is classified as a minor application, OPM should update the Authorization of the major system that hosts SharePoint to account for its security control needs and risks. We also recommend that OPM track SharePoint on its system inventories.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for properly representing the potential security risks the system faces.
2	<b>Finding</b>	<u>Policies and Procedures:</u> OPM has not established policies and procedures specific to SharePoint.
	<b>Recommendation</b>	The OIG recommends that OPM establish policies and procedures to address SharePoint's security controls and the risks associated with operating the software in OPM's production environment.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for documenting information security policies and procedures.

*Continued: Audit of OPM's SharePoint Implementation*

3	<b>Finding</b>	<u>Specialized Training</u> : OPM SharePoint administrators and/or site owners do not receive training specific to SharePoint administration and management.
	<b>Recommendation</b>	The OIG recommends that OPM require employees with administrative or managerial responsibilities over SharePoint to take specialized training related to the software.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.
4	<b>Finding</b>	<u>User Account Provisioning</u> : OPM does not have a formal process in place to document all of the SharePoint user accounts approved and provisioned.
	<b>Recommendation</b>	The OIG recommends that OPM implement formal procedures for requesting and provisioning SharePoint user accounts.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing appropriate access to information systems.
5	<b>Finding</b>	<u>User Account Auditing</u> : As noted above, OPM does not have a formal process in place to document all of the SharePoint user accounts approved and provisioned, and therefore it cannot effectively conduct routine audits to ensure access is being granted, modified, and removed appropriately.
	<b>Recommendation</b>	The OIG recommends that OPM implement a formal process to routinely audit SharePoint user accounts for appropriateness. This audit should include verifying individuals are still active employees or contractors and their level of access is appropriate.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing appropriate access to information systems.
6	<b>Finding</b>	<u>Security Configuration Standards and Audits</u> : OCIO has not documented formal security configuration standards for its SharePoint application.
	<b>Recommendation</b>	The OIG recommends that OPM document approved security configuration settings for its SharePoint application.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that information systems are initially configured in a secure manner.

*Continued: Audit of OPM's SharePoint Implementation*

7	<b>Finding</b>	<u>Security Configuration Standards and Audits</u> : OCIO has not documented formal security configuration standards for its SharePoint application and thereby cannot routinely audit the SharePoint configuration settings against these standards.
	<b>Recommendation</b>	The OIG recommends that OPM implement a process to routinely audit the configuration settings of SharePoint to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that servers are in compliance with approved security settings.
8	<b>Finding</b>	<u>Patch Management</u> : Vulnerability scans revealed several servers missing critical patches released more than 90 days before the scans took place. The OCIO responded that they were aware of the missing patches, but with no test environment to test the patches before being deployed into production SharePoint servers, the decision was made to not apply the critical patches.
	<b>Recommendation</b>	The OIG recommends that OPM implement a process to test patches on its SharePoint servers. Once this process has been implemented, we recommend OPM implement controls to ensure all critical patches are installed on SharePoint servers and databases in a timely manner as defined by OPM policies.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for keeping information systems up-to-date with patches and service packs.



**Title: Federal Information Security Modernization Act Audit FY 2017**  
**Report #: 4A-CI-00-17-020**  
**Date: October 27, 2017**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Information Security Governance</u> : OPM does not have the appropriate resources in place to manage its cybersecurity program.
	<b>Recommendation</b>	The OIG recommends that OPM hire a sufficient number of qualified ISSOs to adequately support all of the agency's major information systems.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security.
2	<b>Finding</b>	<u>Security Assessment and Authorization</u> : OPM is operating production systems that have not been subject to a complete and current Authorization.
	<b>Recommendation</b>	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
3	<b>Finding</b>	<u>Security Assessment and Authorization</u> : OPM is operating production systems that have not been subject to a complete and current Authorization.
	<b>Recommendation</b>	The OIG recommends that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.
	<b>Status</b>	OPM disagreed with this recommendation. However, the agency stated that it will consult with subject matter experts to determine whether and how to implement the recommendation.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
4	<b>Finding</b>	<u>Inventory of Major Systems and System Interconnections</u> : OPM's system inventory does not include all of the system interconnections.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

5	<b>Finding</b>	<u>Inventory of Major Systems and System Interconnections</u> : OPM's system inventory does not include all of the system interconnections.
	<b>Recommendation</b>	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.
6	<b>Finding</b>	<u>Hardware Inventory</u> : OPM's hardware inventory does not contain information that associates hardware components to the major system(s) that they support.
	<b>Recommendation</b>	The OIG recommends that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying and documenting systems and assets.
7	<b>Finding</b>	<u>Software Inventory</u> : OPM's software inventory does not contain the level of detail necessary for thorough tracking and reporting.
	<b>Recommendation</b>	The OIG recommends that OPM define the standard data elements for an inventory of software assets and licenses with the detailed information necessary for tracking and reporting, and that it update its software inventory to include these standard data elements.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for understanding the information assets in the organization's environment.
8	<b>Finding</b>	<u>Risk Policy and Strategy</u> : OPM's Risk Management Council has not yet established an overall risk strategy for the agency.
	<b>Recommendation</b>	The OIG recommends that OPM define and communicate a risk management strategy based on the requirements outlined in NIST SP 800-39.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for properly considering risk information when making investment, security, and operational decisions.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

9	<b>Finding</b>	<u>Information Security Architecture</u> : OPM’s enterprise architecture has not been updated since 2008, and it does not support the necessary integration of an information security architecture.
	<b>Recommendation</b>	The OIG recommends that OPM update its enterprise architecture to include the information security architecture elements required by NIST and OMB guidance.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for aligning the agency’s security processes, systems, and personnel with the agency mission and strategic plan.
10	<b>Finding</b>	<u>Risk Management Roles, Responsibilities, and Resources</u> : OPM’s Risk Management Council is not yet fulfilling all of the responsibilities of the risk executive function required by NIST.
	<b>Recommendation</b>	The OIG recommends that OPM continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing information security risks at OPM.
11	<b>Finding</b>	<u>Plan of Action and Milestones</u> : Over 96 percent of POA&Ms were more than 30 days overdue and over 88 percent were more than 120 days overdue.
	<b>Recommendation</b>	The OIG recommends that OPM adhere to remediation dates for its POA&M weaknesses.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing POA&M weakness remediation.
12	<b>Finding</b>	<u>Plan of Action and Milestones</u> : Over 96 percent of POA&Ms were more than 30 days overdue and over 88 percent were more than 120 days overdue.
	<b>Recommendation</b>	The OIG recommends that OPM update its POA&M entries to reflect both the original and updated remediation deadlines when the control weakness has not been addressed by the originally scheduled deadline (i.e., the POA&M deadline should not reflect a date in the past).
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing POA&M weakness remediation.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

13	<b>Finding</b>	<u>System Level Risk Assessments</u> : A majority of risk assessments for systems that were authorized in FY 2017 had issues with the security control testing and/or the corresponding risk assessment.
	<b>Recommendation</b>	The OIG recommends that OPM complete risk assessments for each major information system that are compliant with NIST guidelines and OPM policy. The results of a complete and comprehensive test of security controls should be incorporated into each risk assessment.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for conducting risk assessments.
14	<b>Finding</b>	<u>Centralized Enterprise-wide Risk Tool</u> : OPM does not have a centralized system or tool to view enterprise-wide risk information, nor has it defined requirements to develop one.
	<b>Recommendation</b>	The OIG recommends that OPM identify and define the requirements for an automated enterprise-wide solution for tracking risks, remediation efforts, dependencies, risk scores, and management dashboards and implement the automated enterprise-wide solution.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for capturing risk information, keeping risk information current, and assessing risk information in aggregate.
15	<b>Finding</b>	<u>System Development Life Cycle</u> : Despite a long history of troubled system development projects, OPM still does not consistently enforce a comprehensive SDLC.
	<b>Recommendation</b>	The OIG recommends that the OCIO develop a plan and timeline to enforce the new SDLC policy on all of OPM's system development projects.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring stability of systems development projects.
16	<b>Finding</b>	<u>Configuration Management (CM) Roles, Responsibilities, and Resources</u> : OPM has indicated that it does not currently have adequate resources (people, processes, and technology) to effectively manage its CM program.
	<b>Recommendation</b>	The OIG recommends that OPM perform a gap analysis to determine the configuration management resource requirements (people, processes, and technology) necessary to effectively implement the agency's CM program.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying gaps in the agency's configuration management program.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

17	<b>Finding</b>	<u>Configuration Management Plan</u> : While OPM does document lessons learned from its configuration change control process, it does not currently use these lessons to update and improve its configuration management plan as necessary.
	<b>Recommendation</b>	The OIG recommends that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for analyzing and updating the agency's configuration management plan.
18	<b>Finding</b>	<u>Configuration Baselines</u> : OPM has not established baseline configurations for all of its information systems.
	<b>Recommendation</b>	The OIG recommends that OPM develop and implement a baseline configuration for all information systems in use by OPM.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that information systems are initially configured in a secure manner.
19	<b>Finding</b>	<u>Configuration Baseline Auditing</u> : OPM has not established baseline configurations for all of its information systems, and therefore is unable to effectively audit its system configurations.
	<b>Recommendation</b>	The OIG recommends that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. This recommendation cannot be addressed until Recommendation 18 has been implemented.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that servers are in compliance with approved security settings.
20	<b>Finding</b>	<u>Security Configuration Settings</u> : OPM has not documented a standard security configuration setting for all of its operating platforms.
	<b>Recommendation</b>	The OIG recommends that the OCIO develop and implement standard security configuration settings for all operating platforms in use by OPM.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that information systems are initially configured in a secure manner.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

21	<b>Finding</b>	<u>Security Configuration Auditing</u> : OPM does not consistently run automated scans to verify that information systems are in compliance with pre-established configuration settings, as they have yet to be developed for all operating platforms.
	<b>Recommendation</b>	The OIG recommends that the OCIO conduct routine compliance scans against the standard security configuration settings for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 20 has been completed.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that servers are in compliance with approved security settings.
22	<b>Finding</b>	<u>Security Configuration Setting Deviations</u> : OPM has not tailored and documented any potential business-required deviations from the configuration standards.
	<b>Recommendation</b>	For OPM configuration standards that are based on a pre-existing generic standard, the OIG recommends that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for secure configuration of information systems.
23	<b>Finding</b>	<u>Flaw Remediation and Patch Management</u> : OPM's scanning tool was unable to successfully scan certain devices within OPM's internal network.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying system vulnerabilities.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

24	<b>Finding</b>	<u>Flaw Remediation and Patch Management</u> : OIG vulnerability scans indicate that OPM’s production environment contains many instances of unsupported software and operating platforms.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for remediating known vulnerabilities.
25	<b>Finding</b>	<u>Flaw Remediation and Patch Management</u> : OPM does not have a process to record or track the remediation status for weaknesses identified during vulnerability scans.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for remediating known vulnerabilities.
26	<b>Finding</b>	<u>Flaw Remediation and Patch Management</u> : OPM does not have a process to record or track the remediation status for weaknesses identified during vulnerability scans.
	<b>Recommendation</b>	The OIG recommends that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for remediating known vulnerabilities.
27	<b>Finding</b>	<u>Identity, Credential, and Access Management (ICAM) Roles, Responsibilities, and Resources</u> : OPM does not have a process in place to ensure that adequate resources (people, processes, and technology) are provided to stakeholders to fully implement ICAM controls.
	<b>Recommendation</b>	The OIG recommends that OPM conduct an analysis to identify limitations in the current ICAM program in order to ensure that stakeholders have adequate resources (people, processes, and technology) to implement the agency’s ICAM activities.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying the necessary resources required to maintain and progress OPM’s ICAM program.



*Continued: Federal Information Security Modernization Act Audit FY 2017*

28	<b>Finding</b>	<u>ICAM Strategy</u> : OPM has not developed an ICAM strategy that includes a review of current practices (“as-is” assessment), identification of gaps (from a desired or “to-be” state), and a transition plan.
	<b>Recommendation</b>	The OIG recommends that OPM develop and implement an ICAM strategy that considers a review of current practices (“as-is” assessment) and the identification of gaps (from a desired or “to-be” state), and contains milestones for how the agency plans to align with Federal ICAM initiatives.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring the success of the agency’s ICAM initiatives.
29	<b>Finding</b>	<u>Implementation of an ICAM Program</u> : OPM has not implemented Personal Identity Verification (PIV) at the application level, and does not adequately manage contractor accounts.
	<b>Recommendation</b>	The OIG recommends that OPM implement a process to capture and share lessons learned on the effectiveness of its ICAM policies, procedures, and processes to update the program.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for implementing the ICAM program with speed and efficiency.
30	<b>Finding</b>	<u>Multi-factor Authentication with PIV</u> : PIV authentication at the application level is only in place for 3 of OPM’s 46 major applications.
	<b>Recommendation</b>	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for authenticating to information systems.
31	<b>Finding</b>	<u>Contractor Access Management</u> : OPM does not maintain a complete list of all contractors who have access to OPM’s network, so there is no way for the OCIO to audit the termination process to ensure that contractor accounts are removed in a timely manner.
	<b>Recommendation</b>	The OIG recommends that the OCIO maintain a centralized list of all contractors that have access to the OPM network and use this list to routinely audit all user accounts for appropriateness.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for limiting inappropriate access to critical or sensitive resources.



*Continued: Federal Information Security Modernization Act Audit FY 2017*

32	<b>Finding</b>	<u>Assessment of Workforce</u> : OPM has not defined a process for conducting an assessment of the knowledge, skills, and abilities of its workforce to determine employees' specialized training needs.
	<b>Recommendation</b>	The OIG recommends that OPM develop and conduct an assessment of its workforce's knowledge, skills and abilities in order to identify any skill gaps and specialized training needs.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring OPM staff is fully prepared to address the security threats facing the agency.
33	<b>Finding</b>	<u>Security Awareness Strategy</u> : OPM has not defined its security awareness and training strategy or created a plan to develop, implement, and maintain a security awareness program tailored to the mission and risk environment.
	<b>Recommendation</b>	The OIG recommends that OPM develop and document a security awareness and training strategy tailored to its mission and risk environment.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for the effectiveness of the agency's overall security training program.
34	<b>Finding</b>	<u>Information Security Continuous Monitoring (ISCM) Roles, Responsibilities, and Resources</u> : The weaknesses that the OIG identified in OPM's ISCM program indicate that the agency does not have adequate resources to effectively implement the activities required by its ISCM strategy and policies. Furthermore, OPM has not implemented a process to identify the ISCM resource gaps it would need to fill in order to effectively implement its ISCM program.
	<b>Recommendation</b>	The OIG recommends that OPM conduct an analysis to identify any resource gaps within its current ISCM program. OPM should use the results of this gap analysis to ensure stakeholders have adequate resources to effectively implement ISCM activities based on OPM's policies and procedures.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for protecting sensitive information.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

35	<b>Finding</b>	<u>Ongoing Security Assessments</u> : The OIG submitted multiple requests for the security control testing documentation for all OPM systems in order to review them for quality and consistency. However, the OIG was only provided evidence that 9 of OPM’s 46 major systems were subject to security controls testing in FY 2017 that complied with OPM’s ISCM submission schedule.
	<b>Recommendation</b>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for implementing the agency’s ISCM strategy and thereby reducing the risk of an attack.
36	<b>Finding</b>	<u>Measuring ISCM Program Effectiveness</u> : OPM has failed to complete the first step necessary to assess the effectiveness of its ISCM program – to collect the necessary baseline data by actually assessing the security controls of its systems.
	<b>Recommendation</b>	The OIG recommends that OPM evaluate qualitative and quantitative performance measures on the performance of its ISCM program once it can consistently acquire security assessment results, as referenced in recommendation 35.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring proper security controls are in place.
37	<b>Finding</b>	<u>Business Impact Analysis (BIA)</u> : OPM has not performed an agency-wide BIA, and therefore, risks to the agency as a whole are not incorporated into the system-level BIAs and/or contingency plans.
	<b>Recommendation</b>	The OIG recommends that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for being able to restore systems based on criticality and, therefore, be able to meet its recovery time objectives and mission.
38	<b>Finding</b>	<u>Contingency Plan Maintenance</u> : In FY 2017, the OIG received evidence that contingency plans exist for only 40 of OPM’s 46 major systems. Of those 40 contingency plans, only 12 had been reviewed and updated in FY 2017.
	<b>Recommendation</b>	We recommend that the OCIO ensure that all of OPM’s major systems have contingency plans in place and that they are reviewed and updated annually.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

*Continued: Federal Information Security Modernization Act Audit FY 2017*

39	<b>Finding</b>	<u>Contingency Plan Testing</u> : Only 5 of the 46 major information systems were subject to an adequate contingency plan test in fiscal year 2017. Furthermore, contingency plans for 11 of 46 major systems have not been tested for 2 years or longer.
	<b>Recommendation</b>	The OIG recommends that OPM test the contingency plans for each system on an annual basis.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for recovering from an unplanned system outage.

**Title: Audit of Information System General and Application Controls at AvMed Health Plan**

**Report #: 1C-ML-00-17-027**

**Date: December 18, 2017**

<b>Rec. #</b>		
6	<b>Finding</b>	<u>Datacenter Physical Access</u> : AvMed's primary and secondary data centers do not require [REDACTED] nor do they [REDACTED].
	<b>Recommendation</b>	The OIG recommends that AvMed implement [REDACTED] and technical controls to [REDACTED] at its primary and secondary datacenters.
	<b>Status</b>	AvMed is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for preventing unauthorized physical access to server hardware and networking equipment.
7	<b>Finding</b>	<u>Network Segmentation</u> : [REDACTED]
	<b>Recommendation</b>	The OIG recommends that AvMed [REDACTED]
	<b>Status</b>	AvMed is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for preventing unauthorized access and compromise of sensitive servers and data.

*Continued: Audit of Information System General and Application Controls at AvMed Health Plan*

12	<b>Finding</b>	<u>OIG Vulnerability Scanning</u> : The OIG identified specific vulnerabilities during credentialed vulnerability and configuration scans of a sample of servers in AvMed’s network environment.
	<b>Recommendation</b>	The OIG recommends that AvMed remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry that was provided to them.
	<b>Status</b>	AvMed is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for preventing exploitation of system weaknesses for malicious purposes.
14	<b>Finding</b>	<u>Security Configuration Auditing</u> : AvMed does not maintain approved security configuration standards for its operating platforms, and therefore it cannot effectively audit its system’s security settings (i.e., there are no approved settings to which to compare the actual settings).
	<b>Recommendation</b>	The OIG recommends that AvMed implement a process to routinely audit the configuration settings of servers to ensure they are in compliance with the approved security configuration standards.
	<b>Status</b>	AvMed is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for ensuring that servers are in compliance with approved security settings.

**Title: OPM's FY 2017 IT Modernization Expenditure Plan**

**Report #: 4A-CI-00-18-022**

**Date: February 15, 2018**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Modernization Strategy</u> : OCIO officials stressed that they were unable to fully define a modernization strategy because of an overall lack of governance and consistent enterprise architecture in the agency.
	<b>Recommendation</b>	The OIG recommends that OPM establish baseline governance and enterprise architecture improvements that can facilitate the planning and execution of a successful IT modernization strategy.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for effectively implementing a comprehensive IT modernization strategy.

*Continued: OPM's FY 2017 IT Modernization Expenditure Plan*

2	<b>Finding</b>	<u>Modernization Strategy</u> : There only appeared to be one or two individuals working on the IT Modernization Expenditure Plan under the direction of the Deputy CIO. The OIG would expect to see an Integrated Project Team, as required by OMB Circular A-11, Part 7, made up of subject matter experts from all of the relevant disciplines intimately involved in such a critical initiative.
	<b>Recommendation</b>	The OIG recommends that OPM's OCIO focus its spending priorities on establishing the necessary governance and enterprise architecture improvements, including an enterprise IT program management office and an enterprise architecture program management office.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for effectively implementing a comprehensive IT modernization strategy.
3	<b>Finding</b>	<u>Modernization Strategy</u> : OPM still does not have a fully developed modernization strategy. The strategy also does not meet the capital planning and investment control (CPIC) requirements in OMB Circular A-11, part 7, which lays out the principles of acquisition and management of capital IT investments.
	<b>Recommendation</b>	The OIG recommends that OPM develop a comprehensive IT modernization strategy with input from the appropriate stakeholders and convene an Integrated Project Team, as required by OMB Circular A-11, Part 7, to manage the overall modernization program and ensure that proper CPIC processes are followed.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for effectively implementing a comprehensive IT modernization strategy.
4	<b>Finding</b>	<u>Modernization Strategy</u> : The OIG believes that OPM's business units continue to have an improper level of influence over IT management, and that the CIO's office does not directly receive the dedicated funding needed to fulfill its mission.
	<b>Recommendation</b>	The OIG recommends that the OPM Director ensure that the CIO has the appropriate level of control over the IT acquisition and budgeting process across all of OPM.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for establishing the proper resources needed for the planning and execution of a successful IT modernization strategy.

**Title: Audit of OPM's Combined Federal Campaign System**  
**Report #: 4A-MO-00-18-004**  
**Date: March 29, 2018**

<b>Rec. #</b>		
2	<b>Finding</b>	<u>Security Assessment Plan and Report</u> : The assessment results table showed that 80 of the 256 controls tested were not fully satisfied. Of these 80 control deficiencies identified, 7 were not appropriately included in the risk assessment of the Security Assessment Report.
	<b>Recommendation</b>	The OIG recommends that OPM perform an analysis to assess the risk of the seven known control deficiencies that were omitted from the risk assessment. The Combined Federal Campaign System (CFCS) risk assessment and POA&Ms should be updated to include all identified weaknesses and their risk levels.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for identifying risk and managing weaknesses.
3	<b>Finding</b>	<u>Overdue POA&amp;Ms</u> : The CFCS has 41 security weaknesses identified on its POA&M, and 40 have scheduled completion dates that are over eight months overdue.
	<b>Recommendation</b>	The OIG recommends that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for managing POA&M weakness remediation.
4	<b>Finding</b>	<u>Configuration Settings</u> : OIG configuration compliance scans found over 100 configuration settings that were not in compliance with the Defense Information Systems Agency's Security Technical Implementation Guide.
	<b>Recommendation</b>	The OIG recommends that OPM work with the FedRAMP Program Management Office to ensure that its Cloud Service Provider apply the approved security configuration settings for the CFCS.
	<b>Status</b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b>Estimated Program Savings</b>	N/A
	<b>Other Nonmonetary Benefit</b>	Improved controls for securely configuration systems.

*Continued: Audit of OPM's Combined Federal Campaign System*

5	<b><i>Finding</i></b>	<u>Flaw Remediation</u> : The results of OIG credentialed vulnerability scans indicate that several servers were missing critical patches that had been released more than 30 days before the scans took place.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM work with the FedRAMP Program Management Office to ensure that its Cloud Service Provider applies system patches in a timely manner and in accordance with policy.
	<b><i>Status</i></b>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls for maintaining current and up-to-date system software.

### III. EXPERIENCE-RATED HEALTH INSURANCE AUDITS

This section describes the open recommendations from audits of experience-rated health insurance carriers that participate in the Federal Employees Health Benefits Program (FEHBP).

<b>Title: Global Audit of Coordination of Benefits for BCBS Plans</b>		
<b>Report #: 1A-99-00-14-046</b>		
<b>Date: July 29, 2015</b>		
<b>Rec. #</b>		
5	<b>Finding</b>	<u>Statistical Review of Incorrectly Coordinated Claims</u> : For certain claims where there were a large number of claims with small payments, the OIG used a statistical sampling methodology to determine the incorrect payment. We projected the sample results to the relevant universe of paid claims and estimate that the BCBS plans incorrectly paid \$4,486,775 in claims that were not properly coordinated with Medicare.
	<b>Recommendation</b>	The OIG recommends that the OPM contracting officer disallow \$4,486,775 for claims that were not paid in good faith and unreasonably charged to the FEHBP.
	<b>Status</b>	OPM partially agreed with \$302,001 and disagreed with \$4,184,774. As of September 30, 2018, OPM has collected \$252,915, allowed \$4,184,774 and there is a remaining receivable of \$49,086.
	<b>Estimated Program Savings</b>	\$302,001
	<b>Other Nonmonetary Benefit</b>	Approving of statistical sampling, results in a long term standard practice to perform additional statistical reviews.

<b>Title: Audit of Health Care Service Corporation</b>		
<b>Report #: 1A-10-17-14-037</b>		
<b>Date: November 19, 2015</b>		
<b>Rec. #</b>		
1	<b>Finding</b>	<u>Veteran Affairs (VA) Claim Review</u> : Our review determined the Health Care Service Corporation (HCSC) incorrectly paid 13,108 VA claims, resulting in overcharges of \$35,562,962 to the FEHBP. For most of these claims, the Plan did not provide documentation to support how the Plan determined that paying these claims using billed charges was cost effective and advantageous to the FEHBP
	<b>Recommendation</b>	We recommend that the contracting officer disallow \$35,562,962 for claim overcharges and verify that the Plan returns all amounts recovered to the FEHBP. Due to the nature of this finding and the substantial amount questioned, the OIG also recommends that the contracting officer contact the Illinois, Montana, and New Mexico VA service areas to discuss a practical approach for recovery of these claims. Based on regulations, the contracting office should not allow the Plan to offset these recoveries against future payments.
	<b>Status</b>	As of September 30, 2018, OPM has collected \$664,130, allowed \$9,043,212 and there is a remaining receivable of \$25,855,620.
	<b>Estimated Program Savings</b>	\$26,519,750
	<b>Other Nonmonetary Benefit</b>	N/A



*Continued: Audit of Health Care Service Corporation*

2	<b>Finding</b>	<u>Veteran Affairs Claim Review</u> : Our review determined HCSC incorrectly paid 13,108 VA claims, resulting in overcharges of \$35,562,962 to the FEHBP. For most of these claims, the Plan did not provide documentation to support how the Plan determined that paying these claims using billed charges was cost effective and advantageous to the FEHBP.
	<b>Recommendation</b>	The OIG recommends that the contracting officer ensure the Plan is properly negotiating and/or contracting reasonable rates with VA providers on behalf of the FEHBP. Additionally, the contracting officer should ensure the Plan updates its policy to limit VA non-par providers to the FEP's non-par rates.
	<b>Status</b>	OPM is still reviewing this recommendation.
	<b>Estimated Program Savings</b>	Unknown – however, improving provider contracted rates should result in increased program savings to health benefit charges, administrative cost and member's cost share for health benefit services.
	<b>Other Nonmonetary Benefit</b>	Improved controls over ensuring VA claims are processed appropriately and strengthen FEHBP's VA provider networks.
4	<b>Finding</b>	<u>Veteran Affairs Claim Review</u> : Our review determined HCSC incorrectly paid 13,108 VA claims, resulting in overcharges of \$35,562,962 to the FEHBP. For most of these claims, the Plan did not provide documentation to support how the Plan determined that paying these claims using billed charges was cost effective and advantageous to the FEHBP.
	<b>Recommendation</b>	Due to the amount of claim overcharges identified in this finding, the OIG recommends that the contracting officer request the Association to perform a risk assessment on the Plan to determine FEP's impact for administrative cost (e.g., cost allocation methods and indirect expenses) and service charge. Any material differences identified should be properly adjusted in the Plan's accounting records and returned to the FEHBP.
	<b>Status</b>	OPM is still reviewing this recommendation
	<b>Estimated Program Savings</b>	Unknown: however, if implemented, this should result in an increased savings from Jan 1, 2012 - Dec 31, 2014.
	<b>Other Nonmonetary Benefit</b>	N/A

**Title: Global Audit of BCBS Claims-to-Enrollment Match**

**Report #: 1A-99-00-15-008**

**Date: January 21, 2016**

<b>Rec. #</b>		
8	<b>Finding</b>	<u>Statistical Review of Member Enrollment Issues</u> : For certain claims where there were a large number of claims with small payments, we used a statistical sampling methodology to determine the incorrect payment. We projected the sample results to the relevant universe of paid claims. We are 95 percent confident that BCBS plans incorrectly paid \$3,207,289 in claims paid to ineligible members.
	<b>Recommendation</b>	OPM agreed with \$556,851 and disagreed with \$2,650,438. The OIG recommends that the contracting officer disallow \$3,207,289 for claims that were not paid in good faith and unreasonably charged to the FEHBP.
	<b>Status</b>	As of September 30, 2018, OPM has collected \$135,202, allowed \$2,650,438 and there is a remaining receivable of \$421,649.
	<b>Estimated Program Savings</b>	\$556,851
	<b>Other Nonmonetary Benefit</b>	Approving of statistical sampling results in a long term standard practice to perform additional statistical reviews.

**Title: Global Audit of Coordination of Benefits for BCBS Plans**

**Report #: 1A-99-00-15-060**

**Date: October 13, 2016**

<b>Rec. #</b>		
3	<b>Finding</b>	<u>Statistical Review of Incorrectly Coordinated Claims</u> : For certain claims where there were a large number of claims with small payments, we used a statistical sampling methodology to determine the incorrect payment. We projected the sample results to the relevant universe of paid claims. We are 95 percent confident that BCBS plans incorrectly paid \$3,415,424 in claims not properly coordinated with Medicare.
	<b>Recommendation</b>	The OIG recommends that the contracting officer disallow \$3,415,424 for claims that were not paid in good faith and unreasonably charged to the FEHBP and verify that the BCBS plans return all amounts recovered to the FEHBP, regardless of the plans' ability to recover the claim payments from the provider..
	<b>Status</b>	As of September 30, 2018, OPM has collected \$214,413 allowed \$3,134,229 and there is a remaining receivable of \$66,782.
	<b>Estimated Program Savings</b>	\$281,195
	<b>Other Nonmonetary Benefit</b>	Approving of statistical sampling results in a long term standard practice to perform additional statistical reviews.

**Title: Audit of BlueCross BlueShield of North Carolina**  
**Report #: 1A-10-33-15-009**  
**Date: November 10, 2016**

<b>Rec. #</b>		
1	<b><i>Finding</i></b>	<u>Veteran Affairs Claims Review</u> : Our review determined that the Plan incorrectly paid 10,622 claims to VA service providers, resulting in overcharges of \$17,652,501 to the FEHBP.
	<b><i>Recommendation</i></b>	The OIG recommends that the contracting officer disallow \$17,652,501 for claim overcharges and verify that the Plan returns all amounts to the FEHBP. Due to regulations, the contracting officer should not allow the Plan to offset any recoveries against future payments, unless approved by a VA official.
	<b><i>Status</i></b>	OPM is still reviewing this recommendation. As of September 30, 2018, no money has been collected.
	<b><i>Estimated Program Savings</i></b>	\$17,652,501
	<b><i>Other Nonmonetary Benefit</i></b>	N/A
2	<b><i>Finding</i></b>	<u>Veteran Affairs Claims Review</u> : We reviewed a sample of claims where the amount paid to VA service providers was greater than or equal to the amount billed by the provider. We consider these claims as high risk for payment errors because paying a claim at or above the billed amount could indicate that the FEHBP did not receive a discount in the pricing of that claim.
	<b><i>Recommendation</i></b>	The OIG recommends that the contracting officer require the Plan to perform a cost analysis using all lines of business (LOBs) and types of services (i.e., inpatient, outpatient, and physician) to determine what rates are reasonable for the FEHBP to obtain and pay VA facilities. Based on this analysis, the OIG recommends the contracting officer provide oversight that the Plan practices due diligence to ensure the Plan contracts equitably to pay VA claims on behalf of the FEHBP.
	<b><i>Status</i></b>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<b><i>Estimated Program Savings</i></b>	Unknown – however, improving provider contracted rates should result in increased program savings to health benefit charges, administrative cost and member’s cost share for health benefit services.
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls over ensuring VA claims are processed appropriately.

*Continued: Audit of BlueCross BlueShield of North Carolina*

<b>Rec. #</b>		
3	<b><i>Finding</i></b>	<u>Veteran Affairs Claims Review</u> : We reviewed a sample of claims where the amount paid to VA service providers was greater than or equal to the amount billed by the provider. We consider these claims as high risk for payment errors because paying a claim at or above the billed amount could indicate that the FEHBP did not receive a discount in the pricing of that claim.
	<b><i>Recommendation</i></b>	The OIG recommends that the contracting officer require the Plan to perform an analysis to determine the extent that the Plan's administrative cost reimbursements were overstated as a result of the overpayment of VA claims. The contracting officer should ensure that the Plan returns all excessive administrative cost reimbursements to the FEHBP.
	<b><i>Status</i></b>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<b><i>Estimated Program Savings</i></b>	Unknown – however, improving provider contracted rates should result in increased program savings to health benefit charges, administrative cost, and member's cost share for health benefit services.
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls over ensuring VA claims are processed appropriately.
4	<b><i>Finding</i></b>	<u>Hospice Claims Review</u> : Our review determined that the Plan incorrectly paid 833 claims for Hospice services, resulting in overcharges of \$964,834 to the FEHBP.
	<b><i>Recommendation</i></b>	The OIG recommends that the contracting officer disallow \$964,834 for claim overcharges and verify that the Plan returns all amounts recovered to the FEHBP.
	<b><i>Status</i></b>	As of September 30, 2018, \$567,768 had been collected and there was a receivable of \$242,831.
	<b><i>Estimated Program Savings</i></b>	\$810,599
	<b><i>Other Nonmonetary Benefit</i></b>	N/A

**Title: Global Audit of Veterans Affairs for BCBS Plans**  
**Report #: 1A-99-00-16-021**  
**Date: February 28, 2018**

<b>Rec. #</b>		
1	<b>Finding</b>	<u>Veteran Affairs Claim Review</u> : Our audit determined that the BCBS plans incorrectly paid 6,989 claims, resulting in \$58,023,161 in overcharges to the FEHBP. The Association and/or BCBS plans paid most of the claims questioned in this report using the full amount billed by the provider, instead of opting to use a lower available rate.
	<b>Recommendation</b>	The OIG recommends that the contracting officer disallow \$58,023,161 for claim overcharges and that all overcharges be returned to the FEHBP, regardless of the BCBS plans' ability to collect the funds from the providers or members.
	<b>Status</b>	As of September 30, 2018, OPM has collected \$2,620,396, allowed \$666,531 and there is a remaining receivable of \$54,736,234.
	<b>Estimated Program Savings</b>	\$57,356,630
	<b>Other Nonmonetary Benefit</b>	N/A
2	<b>Finding</b>	<u>Veteran Affairs Claim Review</u> : Our audit determined that the BCBS plans incorrectly paid 6,989 claims, resulting in \$58,023,161 in overcharges to the FEHBP. The Association and/or BCBS plans paid most of the claims questioned in this report using the full amount billed by the provider, instead of opting to use a lower available rate.
	<b>Recommendation</b>	The OIG recommends that the contracting officer ensure that the Association develops corrective actions for improving the prevention and detection of VA claims that are not reasonably priced and paid by the BCBS plans.
	<b>Status</b>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<b>Estimated Program Savings</b>	Reduce future FEHBP payments over \$20 million a year.
	<b>Other Nonmonetary Benefit</b>	Reduce veteran members' out-of-pocket expense by having lower cost shares.
3	<b>Finding</b>	<u>Veteran Affairs Claim Review</u> : Our audit determined that the BCBS plans incorrectly paid 6,989 claims, resulting in \$58,023,161 in overcharges to the FEHBP. The Association and/or BCBS plans paid most of the claims questioned in this report using the full amount billed by the provider, instead of opting to use a lower available rate.
	<b>Recommendation</b>	The OIG recommends that the contracting officer require the BCBS plans to perform a cost analysis using all lines of business, places of service (i.e., inpatient, outpatient, and physician), and service types to determine what rates are reasonable for the FEHBP to pay VA facilities. Once this analysis is complete, we recommend that the contracting officer require the BCBS plans to pay VA claims using the lower of the VA's reasonable charge or the local plan's allowance that it would pay for the same care or services in the same geographic area, for all VA providers.
	<b>Status</b>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<b>Estimated Program Savings</b>	Reduce future FEHBP payments over \$20 million a year.
	<b>Other Nonmonetary Benefit</b>	Reduce veteran members' out-of-pocket expense by having lower cost shares.

*Continued: Global Audit of Veterans Affairs for BCBS Plans*

<b>Rec. #</b>		
4	<b><i>Finding</i></b>	<u>Veteran Affairs Claim Review</u> : Our audit determined that the BCBS plans incorrectly paid 6,989 claims, resulting in \$58,023,161 in overcharges to the FEHBP. The Association and/or BCBS plans paid most of the claims questioned in this report using the full amount billed by the provider, instead of opting to use a lower available rate.
	<b><i>Recommendation</i></b>	The OIG recommends that the contracting officer require the Association to enhance the FEP Express system to automatically defer VA claims when a local UCR or average market rate has not been provided for non-par VA claims. These system enhancements should ensure that standard quality control reviews for VA claims (i.e., duplicate edits, OBRA 90 pricing) are being properly applied during the pricing of the claim.
	<b><i>Status</i></b>	OPM agreed with \$26,519,750 and disagreed with \$9,043,212. As of September 30, 2018, OPM has collected \$664,130, allowed \$9,043,212 and there is a remaining receivable of \$25,855,620.
	<b><i>Estimated Program Savings</i></b>	Reduce future FEHBP payments over \$20 million a year.
	<b><i>Other Nonmonetary Benefit</i></b>	Reduce veteran members' out-of-pocket expense by having lower cost shares
5	<b><i>Finding</i></b>	<u>Veteran Affairs Claim Review</u> : Our audit determined that the BCBS plans incorrectly paid 6,989 claims, resulting in \$58,023,161 in overcharges to the FEHBP. The Association and/or BCBS plans paid most of the claims questioned in this report using the full amount billed by the provider, instead of opting to use a lower available rate.
	<b><i>Recommendation</i></b>	The OIG recommends that the contracting officer require the Association to develop auditing and/or oversight procedures to monitor the processing of VA claims. These procedures should include ongoing monitoring of changes to the FEP Express System that impact VA claim pricing and ongoing claim cost rate analysis by VA regions and/or provider types.
	<b><i>Status</i></b>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<b><i>Estimated Program Savings</i></b>	Reduce future FEHBP payments over \$20 million a year.
	<b><i>Other Nonmonetary Benefit</i></b>	Reduce veteran members' out-of-pocket expense by having lower cost shares.

**Title: BlueShield of California Access+ HMO**

**Report #: 1D-SI-00-17-022**

**Date: February 28, 2018**

<b>Rec. #</b>		
3	<b>Finding</b>	<b>Pharmacy and Medical Drug Rebates:</b> As of September 30, 2016, the Plan had not returned pharmacy and medical drug rebates, totaling \$2,000,113, to the FEHBP. Also, the Plan untimely returned pharmacy and medical drug rebates, totaling \$7,208,829, to the FEHBP during the audit scope. As a result, we questioned \$2,107,281 for this audit finding, consisting of \$2,000,113 for the questioned pharmacy and medical drug rebates and \$107,168 for lost investment income (LII) on pharmacy and medical drug rebates returned untimely to the FEHBP.
	<b>Recommendation</b>	The OIG recommends that the contracting officer require the Plan to provide evidence or supporting documentation demonstrating that the Plan has implemented the necessary corrective actions to ensure that pharmacy and medical drug rebates are timely returned to the FEHBP.
	<b>Status</b>	The Plan agrees with this procedural recommendation. In an Audit Resolution Letter, dated September 17, 2018, OPM followed-up with the Plan and required the Plan to develop and provide a corrective action plan to ensure that pharmacy and medical drug rebates are timely returned to the FEHBP. (Note: As part of our audit, we verified that the Plan returned the questioned amounts of \$2,107,281 to the FEHBP.)
	<b>Estimated Program Savings</b>	\$2,107,281
	<b>Other Nonmonetary Benefit</b>	Improved procedures by the Plan to ensure that pharmacy and medical drug rebates are timely returned to the FEHBP.

**Title: Global Audit of Coordination of Benefits for BCBS Plans**

**Report #: 1A-99-00-16-062**

**Date: March 15, 2018**

<b>Rec. #</b>		
1	<b>Finding</b>	<b>Global Coordination of Benefits with Medicare Review:</b> BCBS plans incorrectly paid 5,070 claim lines, resulting in overcharges of \$3,657,586 to the FEHBP. These claims should not have been paid because Medicare was primary during the patient's dates of service.
	<b>Recommendation</b>	The OIG recommends that the contracting officer disallow \$3,657,586 for claim overpayments and verify that the BCBS plans return all amounts recovered to the FEHBP, regardless of the plans' ability to recover the claim payments from providers.
	<b>Status</b>	As of September 30, 2018, OPM has collected \$2,873,435 allowed \$390,293 and there is a remaining receivable of \$393,858.
	<b>Estimated Program Savings</b>	\$3,267,293
	<b>Other Nonmonetary Benefit</b>	N/A

*Continued: Global Audit of Coordination of Benefits for BCBS Plans*

<b>Rec. #</b>		
5	<b><i>Finding</i></b>	<b><u>Statistical Review of Incorrectly Coordinated Claims:</u></b> For certain claims where there were a large number of claims with small payments, the OIG used a statistical sampling methodology to determine the incorrect payment. We projected the sample results to the relevant universe of paid claims and estimate that the BCBS plans incorrectly paid \$2,849,253 in claims that were not properly coordinated with Medicare.
	<b><i>Recommendation</i></b>	The OIG recommends that the OPM contracting officer disallow \$2,849,253 for claims that were not paid in good faith and unreasonably charged to the FEHBP.
	<b><i>Status</i></b>	As of September 30, 2018, OPM has collected \$485,001 allowed \$2,317,059 and there is a remaining receivable of \$47,193.
	<b><i>Estimated Program Savings</i></b>	\$532,194
	<b><i>Other Nonmonetary Benefit</i></b>	Approving of statistical sampling results in a long term standard practice to perform additional statistical reviews.



## IV. COMMUNITY-RATED HEALTH INSURANCE AUDITS

This section describes the open recommendations from audits of the community-rated health insurance carriers that participate in the FEHBP.

<b>Title: Audit of HMO Health Ohio</b>		
<b>Report #: 1C-L4-00-16-013</b>		
<b>Date: September 23, 2016</b>		
<b>Rec. #</b>		
1	<b>Finding</b>	<p><u>Defective Pricing</u>: The Certificates of Accurate Pricing that HMO Health Ohio (Plan) signed for contract years 2011 and 2012 were defective. In accordance with Federal regulations, the FEHBP is therefore due a rate reduction for these years. Application of the defective pricing remedy shows that the FEHBP is due a premium adjustment of \$3,177,807.</p> <p>The OIG determined that defective pricing existed in 2011 and 2012 because the Plan improperly calculated its similarly sized subscriber groups' (SSSGs) rates using rating information from its health maintenance organization (HMO) and preferred provider organization (PPO) product lines, resulting in SSSG discounts that were not applied to the FEHBP.</p>
	<b>Recommendation</b>	The OIG recommends that the OPM contracting officer either require the Plan to reimburse the FEHBP \$3,177,807 for defective pricing, or provide sufficient documentation to support the rate build-up for [REDACTED] PPO product's rates in 2011 and 2012 so that the revenue neutrality resulting from the blending of the HMO and PPO rates can be validated.
	<b>Status</b>	OPM is still reviewing this recommendation.
	<b>Estimated Program Savings</b>	\$3,177,807
	<b>Other Nonmonetary Benefit</b>	To ensure that Federal employees and their employing agencies are paying a fair and reasonable price for health coverage.
2	<b>Finding</b>	<p><u>Lost Investment Income</u>: In accordance with the FEHBP regulations and the contract between OPM and the Plan, the FEHBP is entitled to recover lost investment income on the defective pricing findings in contract years 2011 and 2012. The OIG determined that the FEHBP is due \$306,181 for lost investment income, calculated through August 31, 2016.</p>
	<b>Recommendation</b>	The OIG recommends that the OPM that the contracting officer require the Plan to return \$306,181 to the FEHBP for lost investment income, calculated through August 31, 2016. We also recommend that the OPM contracting officer recover lost investment income on amounts due for the period beginning September 1, 2016, until all defective pricing amounts have been returned to the FEHBP.
	<b>Status</b>	OPM is still reviewing this recommendation. In a Resolution Letter dated February 28, 2018, OPM increased the Lost Investment Income due by \$107,582 to account for the interest that had accrued from September 1, 2016, through January 31, 2018.
	<b>Estimated Program Savings</b>	\$413,763
	<b>Other Nonmonetary Benefit</b>	To ensure that the Federal Government receives reimbursement for interest lost on Program funds due to improper payments.

## VI. OTHER INSURANCE AUDITS

This section describes the open recommendations from audits of other benefit and insurance programs, including the Federal Employees Dental/Vision Insurance Program, the Federal Employees Long Term Care Insurance Program, and the Federal Employees Group Life Insurance Program, as well as audits of Pharmacy Benefit Managements (PBMs) that participate in the FEHBP.

<b>Title: Management Alert – OPM’s Procurement Process for Benefit Programs</b> <b>Report #: 4A-RI-16-014</b> <b>Date: October 14, 2015</b>		
Rec. #		
2	<b><i>Finding</i></b>	<b><u>Period of Performance Significantly Exceeded FAR Limits:</u></b> The FSAFEDS contract exceeded a 12-year period, and there were substantial changes to the Government’s program requirements that occurred over the course of the contract’s term. The FAR limits procurement for this type of service to a 5-year performance period. Furthermore, in the absence of a statutory requirement, the contract’s initial term of seven years with an unlimited number of options is adverse to the Government’s best interest because of a lack of built-in competition for enrollees that is inherent in other benefit programs administered by OPM ( <i>i.e.</i> , the Federal Employees Health Benefits Program and the Federal Employee Dental and Vision Insurance Program).
	<b><i>Recommendation</i></b>	The OIG recommends that controls be implemented to ensure that future program procurements follow FAR requirements and that the contracts’ periods of performance adhere to the limits under the FAR.
	<b><i>Status</i></b>	The agency agreed with the recommendation. The OIG has not yet received sufficient evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	Indirect savings - unknown
	<b><i>Other Nonmonetary Benefit</i></b>	Improved controls to ensure compliance with FAR and to enhance procurements integrity within OPM.

**Title: Audit of the Mail Handlers Benefit Plan’s Pharmacy Operations as Administered by CaremarkPCS Health, L.L.C.**

**Report #: 1H-01-00-16-044**

**Date: October 2, 2017**

Rec. #		
1	<b>Finding</b>	Mail Handlers Benefit Plan (Plan) paid \$1,562,397 in pharmacy claims for ■ dependents age 26 or older whose eligibility to participate in the FEHBP could not be supported. We reviewed the pharmacy claims paid for 2012 through 2014 and found that the Plan was unable to provide evidence to support the eligibility of ■ dependents enrolled in the FEHBP past their 26th birthday. There was no disability certification maintained by the Plan or the member was not removed from the FEHBP timely, increasing the risk of overcharges to the FEHBP.
	<b>Recommendation</b>	The OIG recommends that the Plan provide evidence to support that the ■ dependents were eligible to remain enrolled in the FEHBP due to a disability and incapable of self-support, or return \$1,562,397 to the program.
	<b>Status</b>	The Plan agreed that verification of the member eligibility status is necessary, but it disagreed with our assessment that inadequate internal controls resulted in a significant risk of FEHBP overcharges. As of September 30, 2018, OPM has allowed \$749,587, and there is a receivable of \$812,810.
	<b>Estimated Program Savings</b>	\$1,562,397
	<b>Other Nonmonetary Benefit</b>	Improved controls to ensure compliance with FEHBP eligibility requirements.

## VI. EVALUATIONS

This section describes the open recommendations from evaluations reports issued by the OIG.

<b>Title: Evaluation of OPM's Retirement Services' Customer Service Function</b> <b>Report #: 4K-RS-00-16-023</b> <b>Date: September 28, 2016</b>		
Rec. #		
1	<b><i>Finding</i></b>	<u>Retirement Services is Not Providing Timely Responses to Annuitants' Inquiries</u> : The OIG found that Retirement Services is not providing timely responses to customer inquiries. Specifically, LASs are not responsive to messages left in their voice mailboxes and annuitants are having to make multiple attempts to contact RS for a response to their inquiry.
	<b><i>Recommendation</i></b>	The OIG recommends that Retirement Services establish written policies and procedures for LASs to handle annuitants' phone inquiries including guidelines that ensure LASs are retrieving voice messages regularly to avoid full voicemail boxes and returning calls within a specified time frame.
	<b><i>Status</i></b>	The agency partially agreed with this recommendation and is taking corrective action. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	The OIG believes that if LASs are retrieving voice messages regularly to avoid full voicemail boxes and returning calls within a specified time frame, the number of calls to the toll-free number would be reduced and customer satisfaction would improve.
2	<b><i>Finding</i></b>	<u>Retirement Services is Not Providing Timely Responses to Annuitants' Inquiries</u> : The OIG found that Retirement Services is not meeting its goal to respond to all written correspondence.
	<b><i>Recommendation</i></b>	The OIG recommends Retirement Services allocate additional resources to address the backlog of written correspondences.
	<b><i>Status</i></b>	The agency agreed with this recommendation and is taking corrective action. The OIG has not yet received evidence that implementation has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	By addressing the backlog of written correspondences, annuitants written inquires would be answered in a timely manner and customer satisfaction would improve.

**Title: Evaluation Of The U.S. Office Of Personnel Management’s Retirement Services’ Imaging Operations**  
**Report #: 4K-RS-00-17-039**  
**Date: March 14, 2018**

<b>Rec. #</b>		
1	<b><i>Finding</i></b>	<u>Retirement Services’ Policies and Procedures Do Not Reflect Current Operations</u> : Retirement Services is not following the policies and procedures as outlined in its Retirement Operations Imaging Operational Plan. Specifically, (1) personnel position titles have changed, (2) personnel are no longer performing duties such as bundling records and conducting quality reviews of bundles, and (3) RS has not formalized its established quality assurance process for ensuring accuracy within the imaging process.
	<b><i>Recommendation</i></b>	The OIG recommends that Retirement Services update its Retirement Operations Imaging Operational Plan policies and procedures to reflect its current operations, functions and staffing positions. Specifically, RS should outline its internal controls to ensure staff are up-to-date and ensure accurate and quality imaging.
	<b><i>Status</i></b>	The agency agreed with this recommendation and has provided documentation to support the updating of its Retirement Operations Imaging Operational Plan. The OIG is currently reviewing this documentation to determine if Retirement Services has adequately addressed this recommendation.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	The OIG believes that by Retirement Services formalizing its current policies and procedures to include internal controls, operations, and staffing positions, there is a decreased risk of imaging operation personnel not following the correct quality assurance process.
2	<b><i>Finding</i></b>	<u>Quality Assurance Audits Are Not Conducted Periodically</u> – Retirement Services has not conducted a periodic quality assurance audit of its imaged documents since September 2012. RS is non-compliant with its Retirement Operations Imaging Operating Plan, which states that periodic quality assurance audits should be conducted to ensure documents are accurately imaged, and properly stored.
	<b><i>Recommendation</i></b>	The OIG recommends Retirement Services allocate additional resources to address the backlog of written correspondences.
	<b><i>Status</i></b>	The agency agreed with this recommendation and stated it will conduct periodic quality assurance audits as specified in its Retirement Operations Imaging Operating Plan. Retirement Services provided the OIG with documentation to support conducting a quality assurance audit in 2018. The OIG is currently reviewing this documentation to determine Retirement Services is adequately addressed this recommendation.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	The OIG believes that conducting quality assurance audits periodically will ensure Retirement Services is imaging records accurately and of quality.

*Continued: Evaluation Of The U.S. Office Of Personnel Management's Retirement Services' Imaging Operations*

<b>Rec. #</b>		
3	<b><i>Finding</i></b>	<b><u>No Performance Measures to Assess Benefits of Imaging Efforts:</u></b> Retirement Services has not developed any performance indicators that would allow it to measure the progress of its imaging operations in achieving its desired results.
	<b><i>Recommendation</i></b>	The OIG recommends that Retirement Services develop performance measures to determine if its imaging operations is achieving its intended results.
	<b><i>Status</i></b>	The agency agreed with this recommendation and stated that they would determine the appropriate performance measures based on the result of the quality assurance audits. The OIG has not yet received evidence that the implementation of performance measures has been completed.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	The OIG believes that by establishing performance measures to track the efforts of its imaging operations, RS decreases the risk of wasting limited resources on a program that is not meeting its intended purpose

## VII. MANAGEMENT ADVISORIES

This section describes the open recommendations from management advisories issued by the OIG.

<b>Title: Review of OPM’s Non-Public Decision to Prospectively and Retroactively Re-Apportion Annuity Supplements</b> <b>Report #: L-2018-1</b> <b>Date: February 5, 2018</b>		
Rec. #		
1	<b><i>Finding</i></b>	The OIG found that OPM’s recent reinterpretation was incorrect and section 8421 did not mandate that OPM allocate the annuity supplement between an annuitant and a former spouse when the state court order was silent. OPM’s longstanding past practice of not allocating the supplement supports this finding.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM cease implementing the Retirement Insurance Letter (RIL) 2016-12 and OS Clearinghouse 359 memorandum to apply the state court-ordered marital share to Annuity Supplements unless those court orders expressly and unequivocally identify the Annuity Supplement to be apportioned.
	<b><i>Status</i></b>	OPM disagrees with the recommendation and therefore has taken no action.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	OPM’s change in interpretation requires compliance with the Administrative Procedure Act (APA) and providing public notice and an opportunity to comment before OPM makes substantive changes to established rights. In addition, compliance with the recommendation would restore OPM’s compliance with its ministerial obligations of the underlying state court orders that are silent on the apportionment of the Annuity Supplement.
2	<b><i>Finding</i></b>	See number 1.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM take all appropriate steps to make whole those retired law enforcement officers (LEOs) and any other annuitants affected by this re-interpretation. This would include reversing any annuities that were decreased either prospectively or retroactively that involved a state court order that did not expressly address the Annuity Supplement.
	<b><i>Status</i></b>	OPM disagrees with the recommendation and therefore has taken no action.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Compliance with applicable law, including OPM’s own regulations that require it perform ministerial actions only. This would restore faith in the legal system as well as OPM’s fiduciary responsibilities regarding annuities. It would also restore faith in the parties’ previously negotiated property settlements that are reflected in the underlying state court orders.

*Continued: Review of OPM's Non-Public Decision to Prospectively and Retroactively Re-Apportion Annuity Supplements*

3	<b><i>Finding</i></b>	See number 1.
	<b><i>Recommendation</i></b>	The OIG recommends that OPM determine whether it has a legal requirement to make its updated guidance, including Retirement Insurance Letters, publicly available.
	<b><i>Status</i></b>	OPM disagrees with the recommendation and therefore has taken no action.
	<b><i>Estimated Program Savings</i></b>	N/A
	<b><i>Other Nonmonetary Benefit</i></b>	Compliance with applicable law, so that annuitants and their spouses are public notice of this new OPM policy that significantly affects how OPM processes state court orders – and that has resulted in the imposition of unexpected substantive obligations.



# APPENDIX

Below is a chart listing all reports described in this document that, as of September 30, 2018, had open recommendations over six months old.

Internal Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4A-CF-00-08-025	FY 2008 Financial Statements	11/14/2008	6	1	0	\$0
4A-CF-00-09-037	FY 2009 Financial Statements	11/13/2009	5	1	0	\$0
4A-CF-00-10-015	FY 2010 Financial Statements	11/10/2010	7	3	0	\$0
1K-RS-00-11-068	Stopping Improper Payments to Deceased Annuitants	09/14/2011	14	3	0	\$0
4A-CF-00-11-050	FY 2011 Financial Statements	11/14/2011	7	1	0	\$0
4A-CF-00-12-039	FY 2012 Financial Statements	11/15/2012	3	1	0	\$0
1K-RS-00-12-031	OPM's VOIP Interagency Agreement	12/12/2012	2	1	0	\$0
4A-CF-00-13-034	FY 2013 Financial Statements	12/13/2013	1	1	0	\$0
4A-CF-00-14-039	FY 2014 Financial Statements	11/10/2014	4	3	0	\$0
4K-RS-00-14-076	OPM's Compliance with FOIA	03/23/2015	3	2	0	\$0
4A-RS-00-13-033	Assessing Internal Controls over OPM's RES	04/13/2015	7	1	0	\$0
4A-HR-00-13-055	Human Resources Solutions' Pricing Method	06/02/2015	5	1	0	\$0
4A-CF-00-15-027	FY 2015 Financial Statements	11/13/2015	5	5	0	\$0
4K-RS-00-16-024	OPM's Credit Monitoring & Identity Theft	12/02/2015	2	2	0	\$0
4A-CF-00-16-026	FY 2015 IPERA	05/11/2016	6	1	0	\$0
4A-CA-00-15-041	OPM's OPO's Contract Management Process	07/08/2016	6	5	1	\$108,880,417
4A-CF-00-16-030	FY 2016 Financial Statements	11/14/2016	19	15	0	\$0
4A-CF-00-17-012	FY 2016 IPERA	5/11/2017	10	1	0	\$0
4A-OO-00-16-046	OPM's Purchase Card Program	07/07/2017	12	12	0	\$0
4A-CF-00-17-033	OPM's Compliance with DATA Act	11/09/2017	3	3	0	\$0
4A-CF-00-17-028	FY 2017 Financial Statements	11/13/2017	18	18	0	\$0

<i>Internal Audits Continued</i>						
4A-CF-00-15-049	OPM's Travel Card Program	01/16/2018	21	21	0	\$0
4A-OO-00-17-035	OPM's Award of Credit Monitor Contract to ID Experts	02/28/2018	2	2	0	\$0
4A-CF-00-16-055	OPM's Common Services	03/29/2018	5	5	0	\$0
24	<b>Total Reports</b>		173	109	1	\$108,880,417

<b>Information Systems Audits</b>						
<b>Report Number</b>	<b>Name</b>	<b>Date</b>	<b>Total # of Findings</b>	<b># of Open Procedural Findings</b>	<b>Monetary Findings</b>	
					<b># Open</b>	<b>Amount</b>
4A-CI-00-08-022	FISMA FY 2008	09/23/2008	19	2	0	\$0
4A-CI-00-09-031	FISMA FY 2009	11/05/2009	30	2	0	\$0
4A-CI-00-10-019	FISMA FY 2010	11/10/2010	41	2	0	\$0
4A-CI-00-11-009	FISMA FY 2011	11/09/2011	29	3	0	\$0
4A-CI-00-12-016	FISMA FY 2012	11/05/2012	18	4	0	\$0
4A-CI-00-13-021	FISMA FY 2013	11/21/2013	16	5	0	\$0
4A-CI-00-14-015	IT Security Controls OPM's DTP	06/06/2014	6	2	0	\$0
4A-CI-00-14-016	FISMA FY 2014	11/12/2014	29	15	0	\$0
4A-CI-00-15-055	Flash Audit: OPM's Infrastructure Improvement	06/17/2015	2	1	0	\$0
4A-RI-00-15-019	IT Sec. Controls OPM's AHBOSS	07/29/2015	7	4	0	\$0
4A-CI-00-15-011	FISMA FY 2015	11/10/2015	27	16	0	\$0
4A-CI-00-16-037	2nd Status Report: OPM's Infrastructure Improvement	05/18/2016	2	2	0	\$0
4A-CI-00-16-061	Web Application Security Review	10/13/2016	4	4	0	\$0
4A-CI-00-16-039	FISMA FY 2016	11/09/2016	26	21	0	\$0
4A-RS-00-16-035	IT Sec. Controls OPM's FACES	11/21/2016	13	10	0	\$0
4A-CI-00-17-014	OPM's Security Assessment & Authorization	06/20/2017	4	4	0	\$0

<i>Information System Audits Continued</i>						
4A-CF-00-17-043	OPM's CBIS	09/29/2017	7	5	0	\$0
4A-CF-00-17-044	OPM's Federal Financial System	09/29/2017	9	9	0	\$0
4A-CI-00-17-030	OPM's SharePoint Implementation	09/29/2017	8	8	0	\$0
4A-CI-00-17-020	FISMA FY 2017	10/27/17	39	39	0	\$0
1C-ML-00-17-027	ISG&AC @ AvMed Health Plan	12/18/2017	16	4	0	\$0
4A-CI-00-18-022	OPM's FY 2017 IT Modernization Expenditure	02/15/2018	4	4	0	\$0
4A-MO-00-18-004	OPM's Combined Federal Campaign System	03/29/2018	5	4	0	\$0
23	<b>Total Reports</b>		361	170	0	\$0

<b>Experience-Rated Health Insurance Audits</b>						
<b>Report Number</b>	<b>Name</b>	<b>Date</b>	<b>Total # of Findings</b>	<b># of Open Procedural Findings</b>	<b>Monetary Findings</b>	
					<b># Open</b>	<b>Amount</b>
1A-99-00-14-046	Global COB for BCBS Plans	07/29/2015	5	0	1	\$49,086
1A-10-17-14-037	Health Care Service Corporation	11/19/2015	16	2	1	\$25,855,620
1A-99-00-15-008	Global BCBS Claims-to-Enrollment Match	01/21/2016	8	0	1	\$421,649
1A-99-00-15-060	Global COB for BCBS Plans	10/13/2016	3	0	1	\$66,782
1A-10-33-15-009	BCBS of North Carolina	11/10/2016	6	2	2	\$17,895,332
1D-SI-00-17-022	BlueShield of California Access+ HMO	2/28/18	16	1	0	\$0
1A-99-00-16-021	Global VA Claims for BCBS Plans	2/28/18	5	4	1	\$54,736,234
1A-99-00-16-062	Global COB for BCBS Plans	3/15/18	5	0	2	\$441,051
8	<b>Total Reports</b>		64	9	9	\$99,465,754

Community-Rated Health Insurance Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
1C-L4-00-16-013	HMO Health Ohio	09/23/2016	2	0	2	\$3,591,570
1	<b>Total Reports</b>		2	0	2	\$3,591,570

Other Insurance Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4A-RI-00-16-014	OPM's Procurement Process	10/14/2015	4	1	0	\$0
1H-01-00-16-044	Mailhandlers Benefit Plan's Pharmacy Operations	10/2/2017	3	0	1	\$812,810
2	<b>Total Reports</b>		7	1	1	\$812,810

Evaluations						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4K-RS-00-16-023	OPM's Retirement Services' Customer Service	09/28/2016	3	2	0	\$0
4K-RS-00-17-039	OPM's Retirement Services' Imaging Operations	03/14/2018	3	3	0	\$0
2	<b>Total Reports</b>		6	5	0	\$0

Management Advisories						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
L-2018-1	Review of OPM's Non-Public Decision to Re-Apportion Annuity Supplements	2/5/2018	3	3	0	\$0
1	<b>Total Reports</b>		3	3	0	\$0



## **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