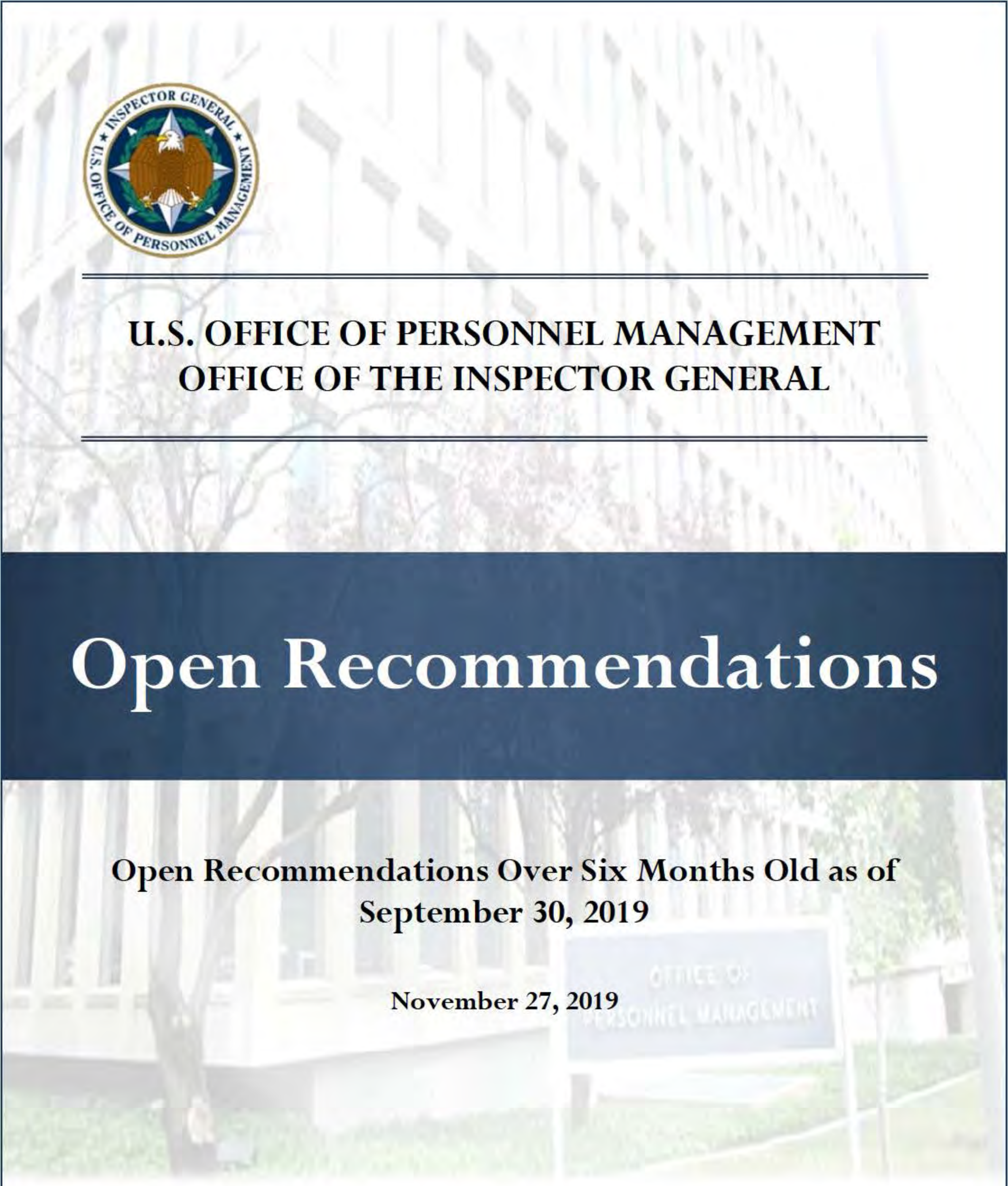

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL

Open Recommendations

Open Recommendations Over Six Months Old as of September 30, 2019

November 27, 2019

EXECUTIVE SUMMARY

Open Recommendations Over Six Months Old as of September 30, 2019

November 27, 2019

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

Norbert E. Vint
Deputy Inspector General Performing the Duties of the Inspector General

As of September 30, 2019 there were 319 unimplemented 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 with Open Recs.	Total # Recs. Made	# Open Recs. as of 9/30/19
Internal Audits	21	184	111
Information Systems Audits	25	415	184
Claim Audits and Analytics	3	27	11
Community-Rated Health Insurance Audits	2	18	5
Other Insurance Audits	1	4	1
Evaluations	3	9	4
Management Advisories	1	3	3
Total	**56**	**660**	**319**

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	110	1	$108.9 M
Information Systems Audits	184	0	$0
Claim Audits and Analytics	8	3	$96.7 M
Community-Rated Health Insurance Audits	3	2	$3.7 M
Other Insurance Audits	1	0	$0
Evaluations	4	0	$0
Management Advisories	3	0	$0
Total	**313**	**6**	**$209.3 M**

**Totals are rounded.*

ABBREVIATIONS

AFR	**Annual Financial Report**
AUP	**Agreed-Upon Procedures**
BCBS	**BlueCross BlueShield**
COB	**Coordination of Benefits**
FAR	**Federal Acquisition Regulation**
FEDVIP	**Federal Employees Dental/Vision Insurance Program**
FEHBP	**Federal Employees Health Benefits Program**
FEP	**BCBS's Federal Employee Program**
FERS	**Federal Employees Retirement System**
FISMA	**Federal Information Security Management Act**
FLTCIP	**Federal Long-Term Care Insurance Program**
FSAFEDS	**Federal Flexible Spending Account Program**
FY	**Fiscal Year**
GSA	**General Services Administration**
HRS	**Human Resources Solutions**
IOC	**OPM's Internal Oversight and Compliance office**
IPERA	**Improper Payments Elimination and Recovery Act**
IT	**Information Technology**
LII	**Lost Investment Income**
N/A	**Not Applicable**
OBRA 90	**Omnibus Budget Reconciliation Act of 1990**
OCFO	**Office of the Chief Financial Officer**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OPM	**U.S. Office of Personnel Management**
OPO	**Office of Procurement Operations**
PBM	**Pharmacy Benefit Manager**
POA&M	**Plan of Action and Milestones**
RS	**Retirement Services**
SAA	**Security Assessment and Authorization**
VA	**U.S. Department of Veterans Affairs**

TABLE OF CONTENTS

Page

I. INTERNAL AUDITS

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

Title: Audit of the Fiscal Year 2008 Financial Statements **Report #: 4A-CF-00-08-025** **Date: November 14, 2008**		
Rec. #1	***Finding***	Information Systems General Control Environment –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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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		
Rec. #1	***Finding***	Information Systems General Control Environment – 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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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		
Rec. #1	***Finding***	Information Systems General Control Environment – 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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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		
Rec. #2	***Finding***	Information Systems General Control Environment – See number 1 above.
	Recommendation	KPMG recommends that the CIO identify common controls, control responsibilities, boundaries and interconnections for information systems in its system inventory.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
Rec. #3	***Finding***	Information Systems General Control Environment – See number 1 above
	Recommendation	KPMG recommends that the CIO implement a process to ensure the POA&Ms remain accurate and complete.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Tracking of Undeliverable IRS Form 1099Rs – OPM does not track undeliverable IRS Form 1099Rs to determine if any annuitants in the population of returned 1099Rs could be deceased.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG is reviewing documentation to determine closure.
	Estimated Program Savings	Potentially significant detection of and reduction in improper payments.
	Other Nonmonetary Benefit	Updated annuity roll records.

Continued: Stopping Improper Payments to Deceased Annuitants		
Rec. #2	***Finding***	Capitalizing on RSM Technology – A modernized environment offers opportunities to reduce instances of fraud, waste, and abuse of the retirement trust fund.
	Recommendation	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.
	Status	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Information Systems Control Environment - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Information Systems Control Environment - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 2013 Financial Statements **Report #: 4A-CF-00-13-034** **Date: December 13, 2013**		
Rec. #1	***Finding***	Information Systems Control Environment - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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		
Rec. #1	***Finding***	Information Systems Control Environment - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
Rec. #2	***Finding***	Information Systems Control Environment - 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.
	Recommendation	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."
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #3	***Finding***	Information Systems Control Environment - The information security control monitoring program was not fully effective in detecting information security control weaknesses. We noted access rights in OPM systems were: • Granted to new users without following the OPM access approval process and quarterly reviews to confirm access approval were not consistently performed. • Not revoked immediately upon user separation and quarterly reviews to confirm access removal were not consistently performed.
	Recommendation	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: • Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process. • 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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #1	***Finding***	Compliance with Electronic Freedom of Information Act Amendments of 1996 (E-FOIA) - 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.
	Recommendation	The OIG recommends that OPM's FOIA Office document a formal policy for handling multiple requests of the same information.
	Status	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing FOIA information requests.

Continued: Audit of OPM's Compliance with the Freedom of Information Act		
Rec. #3	***Finding***	Compliance with Electronic Freedom of Information Act Amendments of 1996: 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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Federal Employees Retirement System Annuity Supplement Surveys and Matches Not Completed - RS has not conducted the 2013 FERS Annuity Supplement Survey and has not performed an annual Annuity Supplement Match since 2009.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 OPM's Fiscal Year 2015 Financial Statements Report #: 4A-CF-00-15-027 Date: November 13, 2015		
Rec. #1	***Finding***	Information Systems Control Environment - The current authoritative guidance regarding two-factor authentication has not been fully applied.
	Recommendation	KPMG recommends that the OCIO fully implement the current authoritative guidance regarding two-factor authentication.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
Rec. #2	***Finding***	Information Systems Control Environment - 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.
	Recommendation	KPMG recommends that the OCIO document and map access rights in OPM systems to personnel roles and functions, following the principle of "least privilege".
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #3	***Finding***	Information Systems Control Environment - The information security control monitoring program was not fully effective in detecting information security control weaknesses. We noted access rights in OPM systems were: • Granted to new users without following the OPM access approval process and quarterly reviews to confirm access approval were not consistently performed. • Not revoked immediately upon user separation and quarterly reviews to confirm access removal were not consistently performed. Granted to a privileged account without following the OPM access approval process.
	Recommendation	KPMG recommends that the OCIO enhance OPM's information security control monitoring program to detect information security control weaknesses by: • Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process; and 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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
Rec. #4	***Finding***	A formalized system component inventory of devices to be assessed as part of vulnerability or configuration management processes was not maintained.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #5	***Finding***	Entity Level Controls Over Financial Management - 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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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: Audit of OPM's Fiscal Year 2015 Improper Payments Reporting
Report #: 4A-CF-00-16-026
Date: May 11, 2016

Rec. #1	***Finding***	Improper Payment Estimates' Root Causes: 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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #2	***Finding***	Inaccurate Contract Amounts Reported in OPM's Information Systems - 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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #3	***Finding***	Weak Controls over the Contract Closeout Process - 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.
	Recommendation	The OIG recommends that OPO develop an accurate inventory of FYs 2013 and 2014 contracts ready for closeout.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #4	***Finding***	Weak Controls over the Contract Closeout Process - See number 3 above.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.

Continued: Audit of OPM's Office of Procurement Operations' Contract Management Process		
Rec. #5	***Finding***	Weak Controls over the Contract Closeout Process - See number 3 above.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #6	***Finding***	Weak Controls over the Contract Closeout Process: 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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	$108,880,417
	Other Nonmonetary Benefit	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.

Title: Audit of OPM's Fiscal Year 2016 Financial Statements **Report #: 4A-CF-00-16-030** **Date: November 14, 2016**		
Rec. #1	***Finding***	Information Systems Control Environment: The Information Security and Privacy Policy Handbook are outdated.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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		
Rec. #2	***Finding***	Information Systems Control Environment: OPM System Documentation is outdated.
	Recommendation	Grant Thornton recommends that OPM create and/or update system documentation as follows: • System Security Plans – Update the plans and perform periodic reviews in accordance with the organization defined frequencies. • Risk Assessments – Conduct a risk assessment for financially relevant applications and systems and a document comprehensive results of the testing performed. • Authority to Operate – Perform security assessment and authorization reviews in a timely manner and create up-to-date packages for systems. • Information System Continuous Monitoring – Document results of continuous monitoring testing performed for systems.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #3	***Finding***	Information Systems Control Environment: The FISMA Inventory Listing is incomplete.
	Recommendation	Grant Thornton recommends that OPM enhance processes in place to track the inventory of the Agency's systems and devices.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #4	***Finding***	Information Systems Control Environment: OPM lacks a system generated listing of terminated agency contractors.
	Recommendation	Grant Thornton recommends that OPM implement a system/control that tracks terminated contractors.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #5	***Finding***	Information Systems Control Environment: Role based training has not been completed.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Individuals obtain skills / training needed to perform day to day duties.
Rec. #7	***Finding***	Information Systems Control Environment: Lack of Monitoring of Plan of Actions and Milestones (POA&Ms)
	Recommendation	Grant Thornton recommends that OPM assign specific individuals with overseeing/monitoring POA&Ms to ensure they are addressed in a timely manner.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #8	***Finding***	Information Systems Control Environment: Lack of periodic access recertifications.
	Recommendation	Grant Thornton recommends that OPM perform a comprehensive review of the appropriateness of personnel with access to systems at the Agency's defined frequencies.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #10	***Finding***	Information Systems Control Environment [redacted] are not PIV compliant.
	Recommendation	Grant Thornton recommends that OPM implement two-factor authentication at the application level in accordance with agency and federal policies.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Two factor authentication will decrease the risk of unauthorized access into OPM systems.
Rec. #11	***Finding***	Information Systems Control Environment: Lack of access descriptions and Segregation of Duties (SoD) Matrices.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #12	***Finding***	Information Systems Control Environment: Access procedures for terminated users are not followed.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Ensuring proper termination procedures are followed will decrease the risk that individuals gain / retain unauthorized access to IT resources/systems.
Rec. #14	***Finding***	Information Systems Control Environment: The FACES audit logs are not periodically reviewed.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #15	***Finding***	Information Systems Control Environment: OPM lacks configuration management policies governing changes to the mainframe environment.
	Recommendation	Grant Thornton recommends that OPM establish a comprehensive configuration management plan that includes roles, responsibilities, and outlines details supporting authorization, testing, and documentation requirements.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #16	***Finding***	Information Systems Control Environment: OPM is unable to generate a complete and accurate listing of modifications to the mainframe and midrange environments.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Decreases the risk that unauthorized or erroneous changes to the mainframe and midrange configuration may be introduced without detection by system owners.
Rec. #17	***Finding***	Information Systems Control Environment: OPM lacks a security configuration checklist
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #19	***Finding***	Monitoring Internal Controls: A-123 Management's Responsibility for Internal Control
	Recommendation	Grant Thornton recommends that OPM strengthen the annual internal assessments, testing, and documentation based on OMB A-123, Appendix A guidance.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Management's inability to conduct a full financial reporting controls assessment could lead to weaknesses in the design and operating effectiveness of financial reporting controls going undetected which could lead to misstatements in OPM's financial statements.

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

Rec. #10	***Finding***	Improper Payment Root Causes: Retirement Services was unable to fully categorize the following improper payments root causes in Table 2, "*Improper Payment Root Cause Category Matrix*," 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. 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."
	Recommendation	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. (Rolled-Forward from FY 2015)
	Status	The agency did not agree with the recommendation. OPM is considering alternative approaches to address the findings. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 Purchase Card Program
Report#: 4A-OO-00-16-046
Date: July 7, 2017

Rec #3	***Finding***	Agency Financial Report: See number 2 above.
	Recommendation	We recommend that the OCFO verify and validate purchase card infurmatin prior to reporting it in the AFR to ensure the integrity of the data reported.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #11	***Finding***	Controls over Purchase Card Transactions: See number 10 above.
	Recommendation	The OIG recommends that that OPO provide documentation for the 17 unsupported transactions identified in Tables 2, 3, and 4.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 OPM's Fiscal Year 2017 Financial Statements
Report #: 4A-CF-00-17-028
Date: November 13, 2017

Rec. #1	***Finding***	System Security Plans, Risk Assessments, Security Assessment and Authorization Packages and Information System Continuous Monitoring documentation were incomplete.
	Recommendation	Grant Thornton recommends that OPM review, update and approve policies and procedures in accordance with frequencies prescribed by OPM policy.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Policies will reflect current operational environment, which will allow personnel to develop and adhere to authorized processes and related controls.
Rec. #2	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 2017 Financial Statements		
Rec. #3	***Finding***	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.
	Recommendation	Grant Thornton recommends that OPM implement processes to associate software and hardware assets to system boundaries.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #4	***Finding***	Instances of applications not scanned during the first quarter of FY 2017 and in July 2017 were noted.
	Recommendation	Grant Thornton recommends that OPM implement backup procedures to ensure continuous security scans over web applications.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #5	***Finding***	OPM did not have a system in place to identify and generate a complete and accurate listing of OPM contractors and their employment status.
	Recommendation	Grant Thornton recommends that OPM implement a system or control that tracks the employment status of OPM contractors.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.

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

Rec. #6	***Finding***	Documentation of the periodic review of POA&Ms did not exist. Several instances of known security weaknesses did not correspond to a POA&M.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The agency is able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.
Rec. #7	***Finding***	OPM did not have a system in place to identify and generate a complete and accurate listing of users with significant information systems responsibilities.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #8	***Finding***	Entity level policies and procedures are outdated and / or incomplete.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 2017 Financial Statements

Rec. #9	***Finding***	OPM did not comply with their policies regarding periodic recertification of the appropriateness of user access.
	Recommendation	Grant Thornton recommends that OPM perform a comprehensive periodic review of the appropriateness of personnel with access to systems.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Two factor authentication will decrease the risk of unauthorized access into OPM systems.
Rec. #10	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Reviews will limit physical security access.
Rec. #11	***Finding***	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.
	Recommendation	Grant Thornton recommends that OPM implement two-factor authentication for applications.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Two factor authentication will decrease the risk of unauthorized access into OPM systems.

Continued: Audit of OPM's Fiscal Year 2017 Financial Statements		
Rec. #12	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #13	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Policies will reflect current operational environment, which will allow personnel to develop and adhere to authorized processes and related controls.
Rec. #14	***Finding***	Security events were not reviewed in a timely manner.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.

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

Rec. #15	***Finding***	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.
	Recommendation	Grant Thornton recommends that OPM establish a means of documenting all users who have access to system.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #16	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Decreases the risk that unauthorized or erroneous changes to the mainframe configuration may be introduced without detection by system owners.
Rec. #17	***Finding***	OPM did not have the ability to generate a complete and accurate listing of modifications made to configuration items to systems.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Decreases the risk that unauthorized or erroneous changes to the mainframe and midrange environments configuration may be introduced without detection by system owners.

Continued: Audit of OPM's Fiscal Year 2017 Financial Statements		
Rec. #18	***Finding***	OPM did not maintain a security configuration checklist for platforms.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Travel Operations lacks clear, concise, and accurate policies and procedures, governing their Travel Charge Card Program.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Current, clear, and accurate policies and procedures will help to reduce the potential for fraud, waste, and abuse of the travel card program.
Rec. #2	***Finding***	See #1 for description.
	Recommendation	The OIG recommends that Travel Operations ensure that roles and responsibilities are clearly articulated to avoid ambiguity of delegated duties.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Consistency creates less confusion among users and increases the accountability between employees and their program managers.

Continued: Audit of OPM's Travel Card Program

Rec. #3	***Finding***	See #1 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not received documentation to show implementation of the recommendation.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Current, clear, and accurate policies and procedures will help to reduce the potential for fraud, waste, and abuse of the travel card program.
Rec. #4	***Finding***	See #1 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Current, clear, and accurate policies and procedures will help to reduce the potential for fraud, waste, and abuse of the travel card program.
Rec. #6	***Finding***	See #5 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Participants that are properly informed of their responsibilities can lead to the decrease in card misuse and abuse.
Rec. #7	***Finding***	See #5 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Properly trained participants can lead to the decrease in card misuse and abuse.

Continued: Audit of OPM's Travel Card Program		
Rec. #8	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Supported transactions decrease the risk for abuse or misuse of the travel card and agency resources.
Rec. #9	***Finding***	See #8 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Supported transactions decrease the risk for abuse or misuse of the travel card and agency resources.
Rec. #10	***Finding***	See #8 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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		
Rec. #11	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #12	***Finding***	See #11 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #13	***Finding***	Travel Operations did not provide support that cardholder accounts with delinquencies of 61 days or more were suspended or cancelled.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Removing cards in the hands of a delinquent cardholder decreases the chances for fraud, misuse, and abuse of the travel card.
Rec. #14	***Finding***	See #13 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Removing cards in the hands of a delinquent cardholder decreases the chances for fraud, misuse, and abuse of the travel card.

Continued: Audit of OPM's Travel Card Program

Rec. #15	***Finding***	Travel Operations did not immediately cancel 176 travel card accounts of employees that separated from OPM.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Cancelling cards immediately upon termination of employment decreases the opportunity for continued use, which can result in travel card misuse and abuse.
Rec. #16	***Finding***	See #15 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Cancelling cards immediately upon termination of employment decreases the opportunity for continued use, which can result in travel card misuse and abuse.
Rec. #17	***Finding***	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.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #18	***Finding***	See #17 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.
Rec. #19	***Finding***	See #17 for description.
	Recommendation	The OIG recommends that Travel Operations establish and implement controls to properly document and retain support for the periodic reviews of inactivity.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.
Rec. #20	***Finding***	Travel Operations does not have controls in place to ensure that the travel card data reported in the Annual Financial Report is accurate.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has received documentation to show implementation of the recommendation; however, based on our review we are still working with the agency to obtain final documentation for closure.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Validating the travel card data ensures the AFR information is not erroneous.

Title: Audit of OPM's Common Services **Report #: 4A-CF-00-16-055** **Date: March 29, 2018**		
Rec. #1	***Finding***	Data Entry Errors were identified in the common services distribution calculation.
	Recommendation	The OIG recommends that the OCFO implement a process to correct identified errors in the same fiscal year.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If effective controls are in place to ensure errors are identified, funding sources will not be incorrectly charged for their share of common services.
Rec. #2	***Finding***	See #1 for description
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM informed us that corrective actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If effective controls are in place to ensure errors are identified, funding sources will not be incorrectly charged for their share of common services.
Rec. #3	***Finding***	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.
	Recommendation	The OIG recommends that the OCFO provide documentation to support the Director's approval of the common services cost.
	Status	The agency agreed with the recommendation. OPM informed us that corrective actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #4	***Finding***	See #3 for description.
	Recommendation	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.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #5	***Finding***	The OCFO's fiscal year 2017 common services bill did not identify the "Unallocated" amount, which is set aside for emergency purposes.
	Recommendation	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.
	Status	The agency did not agreed with the recommendation. Evidence to support their disagreement has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	By providing transparent budget levels, senior official will be aware of all the services that they are being charged for.

Title: Audit of the U.S. Office of Personnel Management's Fiscal Year 2017 Improper Payments Reporting
Report #: 4A-CF-00-18-012
Date: May 10, 2018

Rec. #2	***Finding***	The overall intent of the Improper Payments Information Act of 2002, as amended by IPERA and IPERIA, is to reduce improper payments. While Retirement Services met its improper payment reduction targets for fiscal years 2012 through 2017, Retirement Services' improper payments rate remained basically stagnant during that time period, at roughly an average of 0.37 percent. In addition, Retirement Services' improper payment amounts increased every year from 2012 to their current level of more than $313 million.
	Recommendation	The OIG recommends that Retirement Services develop and implement additional cost effective corrective actions, aimed at the root cause(s) of improper payments, in order to further reduce the improper payments rate.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 Fiscal Year 2018 Financial Statements Report #: 4A-CF-00-18-024 Date: November 15, 2018		
Rec. #1	***Finding***	General Support Systems (GSSs) and application System Security Plans, Risk Assessments, Authority to Operate Packages and Information System Continuous Monitoring documentation were incomplete or not reflective of current operating conditions.
	Recommendation	Grant Thornton recommends that OPM review and update system documentation (System Security Plans and Authority to Operate Packages) and appropriately document results of Risk Assessments and Information System Continuous Monitoring) in accordance with agency policies and procedures.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #2	***Finding***	OPM did not have a centralized process in place to track a complete and accurate listing of systems and devices to be able to provide security oversight or risk mitigation in the protection of its resources.
	Recommendation	Grant Thornton recommends that OPM enhance processes in place to track the inventory of OPM’s systems and devices.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Accurate tracing of OPM’s systems and device inventory will enhance Management’s understand the totality of operational systems/applications within its environment.
Rec. #3	***Finding***	OPM did not have a system in place to identify and generate a complete and accurate listing of OPM contractors and their employment status
	Recommendation	Grant Thornton recommends that OPM implement a system or control that tracks the employment status of OPM contractors.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements

Rec. #4	***Finding***	A complete and accurate listing of Plan of Action and Milestones (POA&Ms) could not be provided. Additionally, documentation of the periodic review of POA&Ms did not exist.
	Recommendation	Grant Thornton recommends that OPM assign specific individuals with overseeing and monitoring POA&Ms to ensure security weaknesses correspond to a POA&M, and are remediated in a timely manner.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The agency will be able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.
Rec. #5	***Finding***	OPM did not have a system in place to identify and generate a complete and accurate listing of users with significant information systems responsibility.
	Recommendation	Grant Thornton recommends that OPM establish a means of documenting a list of users with significant information system responsibilities to ensure the listing is complete and accurate and the appropriate training is completed.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	An accurate listing of users with significant information system responsibility will ensure individuals will obtain skills/training needed to perform day-to-day duties.
Rec. #6	***Finding***	Control owners were unable to articulate the IT internal control environment for one of the six in-scope applications.
	Recommendation	Grant Thornton recommends that OPM conduct a risk assessment to identify current gaps in defining and implementing controls necessary to achieve the NIST baseline for the system. Then, develop, document, and implement controls to achieve full compliance with the baseline.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Implementing controls will ensure that OPM fully complies with the NIST baseline.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements

Rec. #7	***Finding***	Users, including those with privileged access, were not appropriately provisioned and de-provisioned access from OPM's information systems.
	Recommendation	Grant Thornton recommends that OPM ensures 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.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Following and documenting the policies and procedures governing the provisioning and de-provisioning of access to information systems will ensure appropriate access to OPM's information systems.
Rec. #8	***Finding***	OPM did not comply with their policies regarding the periodic recertification of the appropriateness of user access.
	Recommendation	Grant Thornton recommends that OPM perform a comprehensive periodic review of the appropriateness of personnel with access to systems.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Periodic reviews of personnel with access to systems will ensure the appropriateness of user access.
Rec. #9	***Finding***	Physical access to one of the data centers is not appropriate.
	Recommendation	Grant Thornton recommends that OPM ensure policies and procedures governing the provisioning and de-provisioning of access to the data center are followed in a timely manner and documentation of completion of these processes is maintained.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Following and documenting the policies and procedures governing the provisioning and de-provisioning of access to the data center, and implementing physical security access reviews will limit access to appropriate personnel.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements

Rec. #10	***Finding***	Physical access to one of the data centers is not appropriate.
	Recommendation	Grant Thornton also recommends that OPM implement physical security access reviews to ensure access to the data center is limited to appropriate personnel.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Following and documenting the policies and procedures governing the provisioning and de-provisioning of access to the data center. and implementing physical security access reviews will limit access to appropriate personnel.
Rec. #11	***Finding***	Financial applications assessed are 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.
	Recommendation	Grant Thornton recommends that OPM implement two-factor authentication for applications.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Implementing two-factor authentication for applications ensure compliance with OMB-M-11-11 and PIV and OPM policy which requires the two-factor authentication.
Rec. #12	***Finding***	System roles and associated responsibilities or functions, including the identification of incompatible role assignments were not documented.
	Recommendation	Grant Thornton recommends that OPM document access rights to systems to include roles, role descriptions and privileges or activities associated with each role and role or activity assignments that may cause a segregation of duties conflict.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Documenting access rights to OPM systems decreases the risk of systems compromise.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements

Rec. #13	***Finding***	A comprehensive review of audit logs was not performed for the mainframe and four of the six in-scope applications which are mainframe based, or was not performed in a timely manner for one of the six in-scope applications that resides on the network.
	Recommendation	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. Grant Thornton also recommends that OPM establish a means of documenting all users who have access to systems.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Reviewing the audit logs and documenting the review decreases the risk of unauthorized access the mainframe and applications.
Rec. #14	***Finding***	System roles and associated responsibilities or functions, including the identification of incompatible role assignments were not documented.
	Recommendation	Grant Thornton recommends that OPM establish a means of documenting all users who have access to system.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Documenting system roles and responsibilities will ensure access to systems only to authorized users.
Rec. #15	***Finding***	Password and inactivity settings for the general support systems and one of the six in-scope applications are not compliant with OPM policy.
	Recommendation	Grant Thornton recommends that OPM configure password and inactivity parameters to align with agency policies.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Configuring password and inactivity parameters will ensure compliance with OPM policy.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements

Rec. #16	***Finding***	Memorandums of Understandings and Interconnection Service Agreements were not reviewed on an annual basis.
	Recommendation	Grant Thornton recommends that OPM review and update Interagency Service Agreements and Memorandums of Understanding in accordance with agency policies and procedures.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Periodic review of Memorandums of Understandings and Interconnection Service Agreements will increase the understanding of the contents and requirements of the agreements.
Rec. #17	***Finding***	Incident handling procedures were not applied for an event identified within the agency's alert and notification tool.
	Recommendation	Grant Thornton recommends that OPM perform reconciliations to validate that all events noted within the alert and notification tool were appropriately escalated or contained a valid business justification indicating rationale for why escalation is not necessary.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The alert and notification tool will appropriately escalated is necessary.
Rec. #18	***Finding***	OPM had not developed, approved, and disseminated comprehensive configuration management policies and procedures.
	Recommendation	Grant Thornton recommends that OPM establish comprehensive configuration management policies and procedures that include roles and responsibilities and outline details supporting authorization, testing and documentation requirements.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 2018 Financial Statements

Rec. #19	***Finding***	OPM did not have the ability to generate a complete and accurate listing of modifications made to configuration items to the GSS and applications.
	Recommendation	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.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Decreases the risk that unauthorized or erroneous changes to the mainframe and midrange configuration may be introduced without detection by system owners.
Rec. #20	***Finding***	OPM did not maintain a security configuration checklist for platforms.
	Recommendation	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 the settings are appropriate.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #21	***Finding***	Patches were not applied in a timely manner.
	Recommendation	Grant Thornton recommends that OPM establish a process to validate patches, updates, and fixes are applied in a timely manner.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 2018 Financial Statements

Rec. #22	***Finding***	Controls are not in place to validate that data transmitted to applications is complete and accurate.
	Recommendation	Grant Thornton recommends that OPM implement controls to validate that data transmitted to applications is complete and accurate.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Ensures the data transmitted to OPM's applications will be complete and accurate.
Rec. #23	***Finding***	Comprehensive interface/data transmission design documentation is not in place.
	Recommendation	Grant Thornton recommends that OPM develop interface/data transmission design documentation that specifies data fields being transmitted, controls to ensure the completeness and accuracy of data transmitted, and definition of responsibilities.
	Status	The agency agreed with the recommendation. As of September 30, 2019, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Ensures the data transmitted within OPM systems is complete and accurate.

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.

Title: Federal Information Security Management Act Audit FY 2008 **Report #: 4A-CI-00-08-022** **Date: September 23, 2008**		
Rec. #1	***Finding***	Security Controls Testing – 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #2	***Finding***	Contingency Plan Testing – 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.
	Recommendation	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

Title: Federal Information Security Management Act Audit FY 2009 **Report #: 4A-CI-00-09-031** **Date: November 5, 2009**		
Rec. #6	***Finding***	Security Controls Testing: 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.
	Recommendation	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.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Management Act Audit FY 2009		
Rec. #9	***Finding***	Contingency Plan Testing: 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.
	Recommendation	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.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #10	***Finding***	Test of Security Controls: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #30	***Finding***	Contingency Plan Testing: 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.
	Recommendation	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.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #7	***Finding***	Test of Security Controls: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #19	***Finding***	Contingency Plan Testing: 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.
	Recommendation	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.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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, 2012

Rec. #11	***Finding***	Multi-factor Authentication: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.

Continued: Federal Information Security Management Act Audit FY 2012		
Rec. #14	***Finding***	Test of Security Controls: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #15	***Finding***	Contingency Plan Testing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #2	***Finding***	SDLC Methodology: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring stability of systems development projects.

Continued: Federal Information Security Management Act Audit FY 2013

Rec. #11	***Finding***	Multi-factor Authentication: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.
Rec. #13	***Finding***	Test of Security Controls: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #14	***Finding***	Contingency Plan Testing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #4	***Finding***	Configuration Change Control: DTP application programmers have the technical ability to develop a change and move it into production without following the appropriate change control process.
	Recommendation	The OIG recommends that the OCIO make the appropriate system modifications to ensure appropriate segregation of duties are enforced within DTP.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing changes to information systems.
Rec. #5	***Finding***	Configuration Change Control: DTP application programmers have the technical ability to develop a change and move it into production without following the appropriate change control process.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #2	***Finding***	SDLC Methodology: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring stability of systems development projects.

Continued: Federal Information Security Management Act Audit FY 2014

Rec. #3	***Finding***	Security Assessment and Authorization: Eleven OPM systems are operating without an active Security Assessment and Authorization.
	Recommendation	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #4	***Finding***	Security Assessment and Authorization: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #7	***Finding***	Baseline Configurations: 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.
	Recommendation	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]
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.

Continued: Federal Information Security Management Act Audit FY 2014		
Rec. #8	***Finding***	Configuration Auditing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.
Rec. #11	***Finding***	Vulnerability Scanning: 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.
	Recommendation	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for detecting and vulnerabilities.
Rec. #12	***Finding***	Vulnerability Scanning: The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for tracking and remediating vulnerabilities.

Continued: Federal Information Security Management Act Audit FY 2014

Rec. #14	***Finding***	Patching Management: Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for keeping information systems up-to-date with patches and service packs.
Rec. #21	***Finding***	Multi-factor Authentication: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.
Rec. #23	***Finding***	Test of Security Controls: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #24	***Finding***	Contingency Plans: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

Continued: Federal Information Security Management Act Audit FY 2014		
Rec. #25	***Finding***	Contingency Plan Testing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.
Rec. #28	***Finding***	Contractor System Documentation: 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.
	Recommendation	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.
Rec. #29	***Finding***	Contractor System Documentation: 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.
	Recommendation	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #1	***Finding***	Project Management Activities: 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.
	Recommendation	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.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #3	***Finding***	Identification and Authentication (Organizational Users) : 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.
	Recommendation	The OIG recommends that RS require GDIT to enforce PIV authentication for all required AHBOSS users.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and authenticating system users.

Continued: Audit of Information Security Controls of OPM's AHBOSS		
Rec. #4	***Finding***	Physical Access Control: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for physical access the data center.

Title: Federal Information Security Management Act Audit FY 2015 **Report #: 4A-CI-00-15-011** **Date: November 10, 2015**		
Rec. #2	***Finding***	SDLC Methodology: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring stability of systems development projects.
Rec. #3	***Finding***	Security Assessment and Authorization: Eleven OPM systems are operating without an active Security Assessment and Authorization.
	Recommendation	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Management Act Audit FY 2015

Rec. #4	***Finding***	Security Assessment and Authorization: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #7	***Finding***	Test of Security Controls: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #8	***Finding***	Baseline Configurations: 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.
	Recommendation	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]
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.

Continued: Federal Information Security Management Act Audit FY 2015

Rec. #9	***Finding***	Configuration Auditing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.
Rec. #10	***Finding***	Vulnerability Scanning: 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.
	Recommendation	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for detecting and remediating vulnerabilities.
Rec. #11	***Finding***	Vulnerability Scanning: The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for tracking and remediating vulnerabilities.

Continued: Federal Information Security Management Act Audit FY 2015		
Rec. #13	***Finding***	Unsupported Software: The results of our vulnerability scans indicated that OPM's production environment contains severely out-of-date and unsupported software and operating platforms.
	Recommendation	The OIG recommends the OCIO implement a process to ensure that only supported software and operating platforms are utilized within the network environment.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring up-to-date software and operating platforms.
Rec. #14	***Finding***	Patching Management: Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for keeping information systems up-to-date with patches and service packs.
Rec. #16	***Finding***	Multi-factor Authentication: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.

Continued: Federal Information Security Management Act Audit FY 2015

Rec. #24	***Finding***	Contingency Plans: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.
Rec. #25	***Finding***	Contingency Plan Testing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.
Rec. #26	***Finding***	Contractor System Documentation: 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.
	Recommendation	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 2015		
Rec. #27	***Finding***	Contractor System Documentation: 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.
	Recommendation	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Major IT Business Case: 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.
	Recommendation	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).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for minimizing the risk of a major project failure.

Continued: Second Status Report: OPM's Infrastructure Improvement		
Rec. #2	***Finding***	Lifecycle Cost Estimates: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Web Application Inventory: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and documenting web based applications.

Continued: Audit of OPM's Web Application Security Review		
Rec. #2	***Finding***	Policies and Procedures: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for establishing policy and procedures governing the hardening of web applications.
Rec. #3	***Finding***	Web Application Vulnerability Scanning: 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).
	Recommendation	The OIG recommends that OPM implement a process to perform credentialed web application vulnerability scans and track any identified vulnerabilities until they are remediated.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for detecting and tracking vulnerabilities.
Rec. #4	***Finding***	Web Application Vulnerability Scanning: 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.
	Recommendation	The OIG recommends that OPM analyze our scan results to identify false positives and remediate any verified vulnerabilities.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for remediating vulnerabilities.

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

Rec. #1	***Finding***	Security Management Structure: OPM has experienced a high turnover rate for ISSO and CISO positions and has struggled to backfill these vacancies.
	Recommendation	The OIG recommends that OPM hire a sufficient number of ISSOs to adequately support all of the agency's major information systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security.
Rec. #3	***Finding***	SDLC Methodology: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring stability of systems development projects.
Rec. #4	***Finding***	Security Assessment and Authorization: OPM systems are operating without an active Security Assessment and Authorization.
	Recommendation	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #5	***Finding***	Security Assessment and Authorization: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Management Act Audit FY 2016		
Rec. #8	***Finding***	Adherence to Remediation Deadlines: 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.
	Recommendation	The OIG recommends that OPM adhere to remediation dates for its POA&M weaknesses.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing POA&M weakness remediation.
Rec. #9	***Finding***	Contractor System Documentation: 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.
	Recommendation	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.
Rec. #10	***Finding***	Contractor System Documentation: 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.
	Recommendation	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.

Continued: Federal Information Security Management Act Audit FY 2016

Rec. #11	***Finding***	System Inventory: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for oversight, risk management, and securing the agency's information systems.
Rec. #12	***Finding***	Baseline Configurations: 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.
	Recommendation	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]
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #13	***Finding***	Document Deviations to the Standard Configuration Baseline: OPM does not maintain a record of the specific deviations from generic configuration standards.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for effectively auditing a system's actual settings.

Continued: Federal Information Security Management Act Audit FY 2016		
Rec. #14	***Finding***	Vulnerability Scanning: 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.
	Recommendation	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for detecting and remediating vulnerabilities.
Rec. #15	***Finding***	Unsupported Software: The results of our vulnerability scans indicated that OPM's production environment contains severely out-of-date and unsupported software and operating platforms.
	Recommendation	The OIG recommends the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring up-to-date software and operating platforms.
Rec. #16	***Finding***	Configuration Auditing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.

Continued: Federal Information Security Management Act Audit FY 2016		
Rec. #17	***Finding***	Vulnerability Scanning: The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for tracking and remediating vulnerabilities.
Rec. #18	***Finding***	Patching Management: Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for keeping information systems up-to-date with patches and service packs.
Rec. #19	***Finding***	Contractor Access Termination: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing appropriate access to information systems.

Continued: Federal Information Security Management Act Audit FY 2016

Rec. #20	***Finding***	Multi-factor Authentication: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.
Rec. #23	***Finding***	Test of Security Controls: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #25	***Finding***	Contingency Plans: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

Continued: Federal Information Security Management Act Audit FY 2016

Rec. #26	***Finding***	Contingency Plan Testing: FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis.
	Recommendation	The OIG recommends that OPM's program offices test the contingency plans for each system on an annual basis.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #11	***Finding***	[redacted]
	Recommendation	[redacted]
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for adequately segregating the public facing and internal components of FACES.
Rec. #12	***Finding***	[redacted]
	Recommendation	[redacted]
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #1	***Finding***	System Security Plan: The LAN/WAN SSP does not fully and accurately identify all of the security controls applicable to this system.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that system security controls are properly documented.
Rec. #2	***Finding***	System Controls Assessment: The LAN/WAN security controls assessment likely did not identify vulnerabilities that could have been detected with a thorough test.
	Recommendation	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).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #3	***Finding***	Plan of Action and Milestones: OPM was unable to provide a POA&M for the LAN/WAN.
	Recommendation	The OIG recommends that the OCIO update and maintain a complete POA&M list for the LAN/WAN.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for tracking know information security weaknesses.

Continued: Audit of OPM's Security Assessment and Authorization		
Rec. #4	***Finding***	Other Authorization Packages: Many of the Authorization packages completed as part of the Sprint were not complete.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that system risk has been assessed before being approved to operate.

Title: Audit of OPM's Federal Financial System **Report #: 4A-CF-00-17-044** **Date: September 29, 2017**		
Rec. #1	***Finding***	Privacy Impact Assessment (PIA): The Privacy Threshold Analysis and the Privacy Impact Assessment are both incomplete and have not been approved or signed.
	Recommendation	The OIG recommends that OPM fully completes and approves a PIA for BFMS.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying privacy vulnerabilities existing on the information system.
Rec. #7	***Finding***	Overdue Plan of Action and Milestones: A large number of POA&Ms are significantly overdue without revised and approved remediation plans.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for addressing weaknesses in an appropriate timeframe and limiting system exposure to malicious attacks.

Title: Audit of OPM's SharePoint Implementation
Report #: 4A-CI-00-17-030
Date: September 29, 2017

Rec. #1	***Finding***	System Classification: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for properly representing the potential security risks the system faces.
Rec. #2	***Finding***	Policies and Procedures: OPM has not established policies and procedures specific to SharePoint.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for documenting information security policies and procedures.
Rec. #3	***Finding***	Specialized Training: OPM SharePoint administrators and/or site owners do not receive training specific to SharePoint administration and management.
	Recommendation	The OIG recommends that OPM require employees with administrative or managerial responsibilities over SharePoint to take specialized training related to the software.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security risks at OPM.

Continued: Audit of OPM's SharePoint Implementation

Rec. #4	***Finding***	User Account Provisioning: OPM does not have a formal process in place to document all of the SharePoint user accounts approved and provisioned.
	Recommendation	The OIG recommends that OPM implement formal procedures for requesting and provisioning SharePoint user accounts.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing appropriate access to information systems.
Rec. #5	***Finding***	User Account Auditing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing appropriate access to information systems.
Rec. #6	***Finding***	Security Configuration Standards and Audits: OCIO has not documented formal security configuration standards for its SharePoint application.
	Recommendation	The OIG recommends that OPM document approved security configuration settings for its SharePoint application.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #7	***Finding***	Security Configuration Standards and Audits: OCIO has not documented formal security configuration standards for its SharePoint application and thereby cannot routinely audit the SharePoint configuration settings against these standards.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.

Continued: Audit of OPM's SharePoint Implementation		
Rec. #8	***Finding***	Patch Management: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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**		
Rec. #1	***Finding***	Information Security Governance: OPM does not have the appropriate resources in place to manage its cybersecurity program.
	Recommendation	The OIG recommends that OPM hire a sufficient number of qualified ISSOs to adequately support all of the agency's major information systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security.
Rec. #2	***Finding***	Security Assessment and Authorization: OPM is operating production systems that have not been subject to a complete and current Authorization.
	Recommendation	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Modernization Act Audit of FY 2017		
Rec. #3	***Finding***	Security Assessment and Authorization: OPM is operating production systems that have not been subject to a complete and current Authorization.
	Recommendation	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.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #4	***Finding***	Inventory of Major Systems and System Interconnections: OPM's system inventory does not include all of the system interconnections.
	Recommendation	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.
Rec. #5	***Finding***	Inventory of Major Systems and System Interconnections: OPM's system inventory does not include all of the system interconnections.
	Recommendation	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.
Rec. #6	***Finding***	Hardware Inventory: OPM's hardware inventory does not contain information that associates hardware components to the major system(s) that they support.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and documenting systems and assets.

Continued: Federal Information Security Modernization Act Audit FY 2017		
Rec. #7	***Finding***	Software Inventory: OPM's software inventory does not contain the level of detail necessary for thorough tracking and reporting.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for understanding the information assets in the organization's environment.
Rec. #9	***Finding***	Information Security Architecture: OPM's enterprise architecture has not been updated since 2008, and it does not support the necessary integration of an information security architecture.
	Recommendation	The OIG recommends that OPM update its enterprise architecture to include the information security architecture elements required by NIST and OMB guidance.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for aligning the agency's security processes, systems, and personnel with the agency mission and strategic plan.
Rec. #11	***Finding***	Plan of Action and Milestones: Over 96 percent of POA&Ms were more than 30 days overdue and over 88 percent were more than 120 days overdue.
	Recommendation	The OIG recommends that OPM adhere to remediation dates for its POA&M weaknesses.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing POA&M weakness remediation.
Rec. #12	***Finding***	Plan of Action and Milestones: Over 96 percent of POA&Ms were more than 30 days overdue and over 88 percent were more than 120 days overdue.
	Recommendation	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).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing POA&M weakness remediation.

Continued: Federal Information Security Modernization Act Audit FY 2017

Rec. #13	***Finding***	System Level Risk Assessments: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for conducting risk assessments.
Rec. #14	***Finding***	Centralized Enterprise-wide Risk Tool: OPM does not have a centralized system or tool to view enterprise-wide risk information, nor has it defined requirements to develop one.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for capturing risk information, keeping risk information current, and assessing risk information in aggregate.
Rec. #15	***Finding***	System Development Life Cycle: Despite a long history of troubled system development projects, OPM still does not consistently enforce a comprehensive SDLC.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring stability of systems development projects.
Rec. #16	***Finding***	Configuration Management (CM) Roles, Responsibilities, and Resources: OPM has indicated that it does not currently have adequate resources (people, processes, and technology) to effectively manage its CM program.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying gaps in the agency's configuration management program.

Continued: Federal Information Security Modernization Act Audit FY 2017

Rec. #17	***Finding***	Configuration Management Plan: 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.
	Recommendation	The OIG recommends that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for analyzing and updating the agency's configuration management plan.
Rec. #18	***Finding***	Configuration Baselines: OPM has not established baseline configurations for all of its information systems.
	Recommendation	The OIG recommends that OPM develop and implement a baseline configuration for all information systems in use by OPM.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #19	***Finding***	Configuration Baseline Auditing: OPM has not established baseline configurations for all of its information systems, and therefore is unable to effectively audit its system configurations.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.
Rec. #20	***Finding***	Security Configuration Settings: OPM has not documented a standard security configuration setting for all of its operating platforms.
	Recommendation	The OIG recommends that the OCIO develop and implement standard security configuration settings for all operating platforms in use by OPM.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.

Continued: Federal Information Security Modernization Act Audit FY 2017		
Rec. #21	***Finding***	Security Configuration Auditing: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.
Rec. #22	***Finding***	Security Configuration Setting Deviations: OPM has not tailored and documented any potential business-required deviations from the configuration standards.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for secure configuration of information systems.
Rec. #23	***Finding***	Flaw Remediation and Patch Management: OPM's scanning tool was unable to successfully scan certain devices within OPM's internal network.
	Recommendation	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying system vulnerabilities.

Continued: Federal Information Security Modernization Act Audit FY 2017		
Rec. #24	***Finding***	Flaw Remediation and Patch Management: OIG vulnerability scans indicate that OPM's production environment contains many instances of unsupported software and operating platforms.
	Recommendation	The OIG recommends that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for remediating known vulnerabilities.
Rec. #25	***Finding***	Flaw Remediation and Patch Management: OPM does not have a process to record or track the remediation status for weaknesses identified during vulnerability scans.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for remediating known vulnerabilities.
Rec. #26	***Finding***	Flaw Remediation and Patch Management: OPM does not have a process to record or track the remediation status for weaknesses identified during vulnerability scans.
	Recommendation	The OIG recommends that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for remediating known vulnerabilities.
Rec. #27	***Finding***	Identity, Credential, and Access Management (ICAM) Roles, Responsibilities, and Resources: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #28	***Finding***	ICAM Strategy: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring the success of the agency's ICAM initiatives.
Rec. #29	***Finding***	Implementation of an ICAM Program: OPM has not implemented Personal Identity Verification (PIV) at the application level, and does not adequately manage contractor accounts.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for implementing the ICAM program with speed and efficiency.
Rec. #30	***Finding***	Multi-factor Authentication with PIV: PIV authentication at the application level is only in place for 3 of OPM's 46 major applications.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.
Rec. #31	***Finding***	Contractor Access Management: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for limiting inappropriate access to critical or sensitive resources.

Continued: Federal Information Security Modernization Act Audit FY 2017

Rec. #32	***Finding***	Assessment of Workforce: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring OPM staff is fully prepared to address the security threats facing the agency.
Rec. #34	***Finding***	Information Security Continuous Monitoring (ISCM) Roles, Responsibilities, and Resources: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for protecting sensitive information.
Rec. #35	***Finding***	Ongoing Security Assessments: 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.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for implementing the agency's ISCM strategy and thereby reducing the risk of an attack.

Continued: Federal Information Security Modernization Act Audit FY 2017		
Rec. #36	***Finding***	Measuring ISCM Program Effectiveness: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring proper security controls are in place.
Rec. #37	***Finding***	Business Impact Analysis (BIA): 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.
	Recommendation	The OIG recommends that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for being able to restore systems based on criticality and, therefore, be able to meet its recovery time objectives and mission.
Rec. #38	***Finding***	Contingency Plan Maintenance: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.
Rec. #39	***Finding***	Contingency Plan Testing: 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.
	Recommendation	The OIG recommends that OPM test the contingency plans for each system on an annual basis.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

Title: OPM's FY 2017 IT Modernization Expenditure Plan
Report#: 4A-CI-00-18-022
Date: February 15, 2018

Rec. #1	***Finding***	Modernization Strategy: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for effectively implementing a comprehensive IT modernization strategy.
Rec. #2	***Finding***	Modernization Strategy: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for effectively implementing a comprehensive IT modernization strategy.
Rec. #3	***Finding***	Modernization Strategy: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for effectively implementing a comprehensive IT modernization strategy.

Continued: OPM's FY 2017 IT Modernization Expenditure Plan

Rec. #4	***Finding***	Modernization Strategy: 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.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for establishing the proper resources needed for the planning and execution of a successful IT modernization strategy.

Title: Audit of OPM's USA Staffing System
Report #: 4A-HR-00-18-013
Date: May 10, 2018

Rec. #3	***Finding***	Unapproved Configuration Deviations: Configuration deviations for the USA Staffing System have not been documented and approved.
	Recommendation	We recommend that OPM apply the approved security configuration settings for the USA Staffing System.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for reducing system weaknesses.
Rec. #4	***Finding***	Missing Patches: Several of the USA Staffing System servers were missing patches more than 30 days old.
	Recommendation	We recommend that OPM apply system patches in a timely manner and in accordance with policy.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for reducing system weaknesses.

Title: OPM's FY 2018 IT Modernization Expenditure Plan
Report #: 4A-CI-00-18-044
Date: June 20, 2018

Rec. #1	***Finding***	Unnecessary Projects Targeted: Some of the targeted projects included in OPM's FY 2018 spending plan are not strictly necessary and should not be included in the funding.
	Recommendation	We recommend that the OPM Director ensure that the distribution of FY 2018 IT modernization funds is consistent with strengthening OPM's legacy IT environment, as expressed in the FY 2018 Consolidated Appropriations Act.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for meeting the explicit requirements of the FY 2018 Consolidated Appropriations Act.
Rec. #2	***Finding***	Unrelated Projects: Business modernization includes several projects that seem unrelated to the intent of Congressional appropriators.
	Recommendation	We recommend that funding for the FEHBP Central Enrollment Database, the Employee Digital Record, and the Consolidated Business Information System migration be obtained using the normal budget process (or other potential sources, such as the Modernizing Government Technology fund), and not from the FY 2018 IT modernization funds.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for meeting the explicit requirements of the FY 2018 Consolidated Appropriations Act.

Title: Audit of OPM's Health Claims Data Warehouse
Report #: 4A-PP-00-18-011
Date: June 25, 2018

Rec. #2	***Finding***	Outdated SSP: The current HCDW SSP, signed in November 2015, does not adequately reflect the system's current state.
	Recommendation	We recommend that OPM ensure a full independent security controls assessment of the HCDW is conducted based on an updated Security Assessment Plan.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for properly implementing controls to address risk to the system and to OPM as a whole.
Rec. #8	***Finding***	Security Training Records: OPM documents the completion of OPM's annual security awareness training for all HCDW users. However, OPM does not document, monitor, or maintain specialized training specific to HCDW users and account managers.
	Recommendation	We recommend that OPM document specialized training requirements and ensure HCDW users and account managers complete those requirements.

Rec. #8 cont.	***Status***	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security risks at OPM.

Title: Federal Information Security Modernization Act Audit FY 2018
Report #: 4A-CI-00-18-038
Date: October 30, 2018

Rec. #1	***Finding***	Information Security Governance Program: OPM does not have the appropriate resources in place to manage its cybersecurity program.
	Recommendation	We recommend that the OPM Director ensure that the OCIO has sufficient resources to adequately operate, secure, and modernize agency IT systems. We also recommend that the agency hire a sufficient number of Information System Security Officers (ISSOs) to adequately support all of the agency's major information systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security.
Rec. #3	***Finding***	Security Assessment and Authorization: Many authorization packages reviewed were not in compliance with NIST requirements. In some cases, the OCIO issued short-term or interim ATOs in violation of OMB guidance.
	Recommendation	We recommend that all active systems in OPM's inventory have a complete and current Authorization.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #4	***Finding***	Security Assessment and Authorization: Many authorization packages reviewed were not in compliance with NIST requirements. In some cases, the OCIO issued short-term or interim ATOs in violation of OMB guidance.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #5	***Finding***	Inventory of Major Systems: The current policy and procedures for defining system boundaries and classifying systems does not appear to contain a sufficient level of detail to be consistently enforced. As a result, there are systems in the production environment currently in a state of limbo without a defined boundary, classification, or Authorization.
	Recommendation	We recommend that OPM improve the policies and procedures for defining system boundaries and classifying the systems in its environment.
	Status	OPM disagreed initially, but subsequently agreed to the recommendation when it was re-issued in the Federal Information Security Modernization Act Audit of FY 2019. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for properly containing, sharing, and protecting sensitive information.
Rec. #6	***Finding***	Inventory of Major Systems and System Interconnections: The current policy and procedures for defining system boundaries and classifying systems does not appear to contain a sufficient level of detail to be consistently enforced. As a result, there are systems in the production environment currently in a state of limbo without a defined boundary, classification, or Authorization.
	Recommendation	We recommend that the OCIO ensure that all interconnection security agreements are valid and properly maintained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.
Rec. #7	***Finding***	Inventory of Major Systems and System Interconnections: The current policy and procedures for defining system boundaries and classifying systems does not appear to contain a sufficient level of detail to be consistently enforced. As a result, there are systems in the production environment currently in a state of limbo without a defined boundary, classification, or Authorization.
	Recommendation	We recommend that the OCIO ensure that a valid memorandum of understanding/agreement exists for every interconnection.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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 2018

Rec. #8	***Finding***	Hardware Inventory: OPM's hardware inventory includes many of the required elements, but it does not contain information that associates hardware components to the major system(s) that they support.
	Recommendation	We recommend that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and documenting systems and assets.
Rec. #9	***Finding***	Software Inventory: OPM no longer has a centralized software inventory. Instead, OPM now tracks software information at the system level.
	Recommendation	We recommend that OPM define policies and procedures for a centralized software inventory.
	Status	OPM disagreed initially, but subsequently agreed to the recommendation when it was re-issued in the Federal Information Security Modernization Act Audit of FY 2019. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for understanding the information assets in the organization's environment.
Rec. #10	***Finding***	Software Inventory: OPM no longer has a centralized software inventory. Instead, OPM now tracks software information at the system level.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for understanding the information assets in the organization's environment.
Rec. #12	***Finding***	Information Security Architecture: Efforts are underway to begin developing an enterprise architecture, but projected completion dates are well into FY 2019.
	Recommendation	We recommend that OPM update its enterprise architecture to include the information security architecture elements required by NIST and OMB guidance.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for aligning the agency's security processes, systems, and personnel with the agency mission and strategic plan.

Continued: Federal Information Security Modernization Act Audit FY 2018		
Rec. #14	***Finding***	Plan of Action and Milestones: Over 81 percent of POA&Ms were more than 30 days overdue, and over 68 percent of POA&Ms are more than 120 days overdue.
	Recommendation	We recommend that OPM adhere to remediation dates for its POA&M weaknesses.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing POA&M weakness remediation.
Rec. #15	***Finding***	Plan of Action and Milestones: Over 81 percent of POA&Ms were more than 30 days overdue, and over 68 percent of POA&Ms are more than 120 days overdue.
	Recommendation	We recommend that OPM update the remediation deadline in its POA&Ms 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 and the original due should be maintained to track the schedule variance).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	I Improved controls for managing POA&M weakness remediation.
Rec. #16	***Finding***	System Level Risk Assessments: Of the 23 system Authorization packages requested this fiscal year, complete risk assessments were not provided for 11, and widespread issues were noted with the security controls testing and/or the corresponding risk assessment.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for conducting risk assessments.
Rec. #17	***Finding***	Centralized Enterprise-wide Risk Tool: OPM does not have a centralized system or tool to view enterprise-wide risk information.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for capturing current enterprise risk information and assessing it in aggregate.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #18	***Finding***	System Development Life Cycle: Despite a long history of troubled system development projects, OPM still does not consistently enforce a comprehensive SDLC.
	Recommendation	We continue to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy on all of OPM's system development projects.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring stability of systems development projects.
Rec. #19	***Finding***	Configuration Management Roles, Responsibilities, and Resources: OPM has indicated that it does not currently have adequate resources (people, processes, and technology) to effectively manage its CM program.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying gaps in the agency's configuration management program.
Rec. #20	***Finding***	Configuration Management Plan: While the agency 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.
	Recommendation	We recommend that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for analyzing and updating the agency's configuration management plan.
Rec. #21	***Finding***	Baseline Configurations: OPM has not developed a baseline configuration for all of its information systems.
	Recommendation	We recommend that OPM develop and implement a baseline configuration for all information systems in use by OPM.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #22	***Finding***	Baseline Compliance Scanning: OPM does not currently run baseline configuration checks to verify that information systems are in compliance with pre-established baseline configurations, as they have yet to be developed.
	Recommendation	We recommend that the OCIO conduct routine compliance scans against established baseline configurations for all OPM information systems. This recommendation cannot be addressed until Recommendation 21 has been implemented.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.
Rec. #23	***Finding***	Security Configuration Settings: While OPM has workstation and server build images that leverage common best-practice configuration setting standards, it has yet to document and approve standard security configuration settings for all of its operating platforms nor any potential business-required deviations from these configuration standards.
	Recommendation	We recommend that the OCIO develop and implement [standard security configuration settings] for all operating platforms in use by OPM.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #24	***Finding***	Security Configuration Settings: Without formally documented and approved configuration settings, OPM cannot consistently run automated scans to verify that information systems maintain compliance with the pre-established configuration settings.
	Recommendation	We recommend 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 23 has been completed.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #25	***Finding***	Security Configuration Settings: While OPM has workstation and server build images that leverage common best-practice configuration setting standards, it has yet to document and approve standard security configuration settings for all of its operating platforms nor any potential business-required deviations from these configuration standards.
	Recommendation	For OPM configuration standards that are based on a pre-existing generic standard, we recommend that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for secure configuration of information systems.
Rec. #26	***Finding***	Flaw Remediation and Patch Management: Not every device on OPM's network is scanned routinely, nor is there a formal process in place to ensure that all new devices on the agency's network are included in the scanning process.
	Recommendation	We recommend that the OCIO implement a process to ensure new server installations are included in the scan repository.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and remediating system vulnerabilities.
Rec. #28	***Finding***	Flaw Remediation and Patch Management: OPM's scanning tool was unable to successfully scan certain devices within OPM's internal network.
	Recommendation	We recommend that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	Status	OPM disagreed initially, but subsequently agreed to the recommendation when it was re-issued in the Federal Information Security Modernization Act Audit of FY 2019. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and remediating system vulnerabilities.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #29	***Finding***	Flaw Remediation and Patch Management: The results of our independent vulnerability scans indicate that OPM's production environment contains many instances of unsupported software and operating platforms.
	Recommendation	We recommend that the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and remediating system vulnerabilities.
Rec. #30	***Finding***	Flaw Remediation and Patch Management: OPM does not have a process to record or track the remediation status for weaknesses identified during vulnerability scans.
	Recommendation	We recommend that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and remediating system vulnerabilities.
Rec. #31	***Finding***	Flaw Remediation and Patch Management: The results of our independent vulnerability scans indicate that OPM's production environment contains many instances of unsupported software and operating platforms.
	Recommendation	We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and remediating system vulnerabilities.
Rec. #32	***Finding***	ICAM Roles, Responsibilities, and Resources: The OCIO has lost multiple key personnel in FY 2018 and has many vacant ISSO positions. As such, OPM does not have adequate resources (people, processes, and technology) in place to fully implement ICAM controls.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying the necessary resources required to maintain and progress OPM's ICAM program.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #33	***Finding***	ICAM Strategy: 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.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring the success of the agency's ICAM initiatives.
Rec. #34	***Finding***	Implementation of an ICAM Program: OPM policies do not address the capturing and sharing of lessons learned on the effectiveness of the agency's ICAM program.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for implementing the ICAM program with speed and efficiency.
Rec. #35	***Finding***	Multi-factor Authentication with PIV: OPM has not enforced PIV authentication to the vast majority of its applications.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for implementing the ICAM program with speed and efficiency.
Rec. #36	***Finding***	ICAM Contractor Access Management: 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.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for preventing inappropriate access to critical or sensitive resources.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #37	***Finding***	Data Protection and Privacy Policies and Procedures: There is an inadequate number of staff currently within OPM's privacy program. OPM's privacy program is supported by the Chief Privacy Officer, and two detailees from the OCIO. The Chief Privacy Officer position was established in October of 2016. Additional roles and responsibilities needed have not been clearly defined to support the program.
	Recommendation	We recommend that OPM define the roles and responsibilities necessary for the implementation of the agency's privacy program.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for preventing data loss and mishandling of sensitive information.
Rec. #38	***Finding***	Data Protection and Privacy Policies and Procedures: The OPM Information Security and Privacy Policy Handbook is OPM's primary source for data protection and privacy policies. However, this handbook has not been updated since 2011 and does not contain the personally identifiable information (PII) protection plans, policies, and procedures necessary for a mature privacy program.
	Recommendation	We recommend that OPM develop its privacy program by creating the necessary plans, policies, and procedures for the protection of PII.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for preventing data loss and mishandling of sensitive information.
Rec. #42	***Finding***	Data Breach Response Plan: OPM does not currently conduct routine table-top exercises to test the Data Breach Response Plan.
	Recommendation	We recommend that OPM develop a process to routinely test the Data Breach Response Plan.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for preventing major data loss in the event of a security incident.
Rec. #43	***Finding***	Privacy Awareness Training: Individuals with responsibilities for PII or activities involving PII do not receive elevated role-based privacy training.
	Recommendation	We recommend that OPM identify individuals with heightened responsibility for PII and provide role-based training to these individuals at least annually.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for properly handling secure data and preventing data loss incidents.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #44	***Finding***	Assessment of Workforce: Since FY 2017, OPM has conducted an assessment of the knowledge, skills, and abilities of its workforce to determine employees' specialized training needs. While progress has been made, OPM still needs to analyze the results of the assessment to determine any skill gaps and specialized training needs.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that OPM staff are fully prepared to address the security threats facing the agency.
Rec. #46	***Finding***	ISCM Roles, Responsibilities, and Resources: OPM's ISCM program still does not have adequate resources to effectively implement the activities required. This year, OPM made some progress identifying resource gaps related to its ISCM program. However, more work is still required to identify all of the ISCM resource gaps to effectively implement its ISCM program.
	Recommendation	We recommend 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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for effectively implementing the agency's ISCM program, improving its ability to protect sensitive information.
Rec. #47	***Finding***	Ongoing Security Assessments: We continue to find that many system owners are not following the security control testing schedule that the OCIO mandated for all systems. In the first two quarters of 2018, only 29 of OPM's 54 major systems were subject to security controls testing that complied with OPM's ISCM submission schedule. In addition, we were not provided any evidence for the third quarter.
	Recommendation	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for implementing the agency's ISCM strategy and thereby reducing the risk of an attack.

Continued: Federal Information Security Modernization Act Audit FY 2018

Rec. #48	***Finding***	Measuring ISCM Program Effectiveness: OPM still needs to define the format and frequency of reports measuring its ISCM program effectiveness. In addition, 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.
	Recommendation	We recommend 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 47.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring proper security controls are in place.
Rec. #49	***Finding***	Contingency Planning Roles and Responsibilities: OPM's personnel limitations are further evident in OPM's inability to perform all contingency planning activities.
	Recommendation	We recommend that OPM perform a gap analysis to determine the contingency planning requirements (people, processes, and technology) necessary to effectively implement the agency's contingency planning policy.
	Status	OPM disagreed initially, but subsequently agreed to the recommendation when it was re-issued in the Federal Information Security Modernization Act Audit of FY 2019. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for being able to restore systems to an operational status in the event of a disaster.
Rec. #50	***Finding***	Business Impact Analysis: 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.
	Recommendation	We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for being able to restore systems based on criticality and therefore meet its recovery time objectives and mission.

Continued: Federal Information Security Modernization Act Audit FY 2018		
Rec. #51	***Finding***	Contingency Plan Maintenance: In FY 2018, we received evidence that a contingency plan exists for 32 of OPM's 54 major systems. However, of those 33 contingency plans, only 19 were current, having been reviewed and updated in FY 2018.
	Recommendation	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.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.
Rec. #52	***Finding***	Contingency Plan Testing: Only 13 of the 54 major information systems were subject to an adequate contingency plan test in fiscal year 2018. Furthermore, contingency plans for 17 of the 54 major systems have not been tested for 2 years or longer.
	Recommendation	We recommend that OPM test the contingency plans for each system on an annual basis.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

Title: Audit of Information Systems General and Application Controls at Medical Mutual of Ohio
Report #: 1C-UX-00-18-019
Date: January 24, 2019

Rec. #4	***Finding***	[redacted]
	Recommendation	We recommend that Medical Mutual [redacted]
	Status	MMO is taking corrective actions. The OIG has not yet received evidence that implementation has been completed
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for protecting sensitive servers and data from a compromise of a user's system.
Rec. #5	***Finding***	[redacted]
	Recommendation	We recommend that Medical Mutual implement [redacted]
	Status	MMO is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for preventing unauthorized users or devices from connecting to sensitive network resources.
Rec. #10	***Finding***	Security Configuration Auditing: Medical Mutual [redacted]
	Recommendation	We recommend that Medical Mutual implement a process to [redacted] Note - This recommendation cannot be implemented until the controls from Recommendation 9 are in place.
	Status	MMO is taking corrective actions. The OIG has not yet received evidence that implementation has been completed
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are appropriately configured, preventing potential gateways for unauthorized access or malicious activity.

III. CLAIM AUDITS AND ANALYTICS

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

Title: Audit of Health Care Service Corporation **Report #: 1A-10-17-14-037** **Date: November 19, 2015**		
Rec. #1	***Finding***	Veteran Affairs (VA) Claim Review: 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
	Recommendation	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.
	Status	As of September 30, 2019, OPM has collected $664,130, allowed $10,177,287 and there is a remaining receivable of $24,721,545. OPM also provided a draft memo dated September 12, 2019, with their current position on the remaining questioned amount. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	$24,721,545
	Other Nonmonetary Benefit	N/A
Rec. #2	***Finding***	Veteran Affairs Claim Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a draft memo dated September 12, 2019, with their current position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	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.
	Other Nonmonetary Benefit	Improved controls over ensuring VA claims are processed appropriately and strengthen FEHBP's VA provider networks.

Continued: Audit of Health Care Service Corporation

Rec. #4	***Finding***	Veteran Affairs Claim Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a memo dated September 12, 2019, with their position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	Unknown: however, if implemented, this should result in an increased savings from Jan 1, 2012 - Dec 31, 2014.
	Other Nonmonetary Benefit	N/A

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

Rec. #1	***Finding***	Veteran Affairs Claims Review: 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.
	Recommendation	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.
	Status	OPM is still reviewing this recommendation. As of September 30, 2018, no money has been collected. OPM also provided a draft memo dated September 12, 2019, with their current position on the remaining questioned amount. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	$17,652,501
	Other Nonmonetary Benefit	N/A

Continued: Audit of BlueCross BlueShield of North Carolina		
Rec. #2	***Finding***	Veteran Affairs Claims Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a memo dated September 12, 2019, with their position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	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.
	Other Nonmonetary Benefit	Improved controls over ensuring VA claims are processed appropriately.
Rec. #3	***Finding***	Veteran Affairs Claims Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a memo dated September 12, 2019, with their position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	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.
	Other Nonmonetary Benefit	Improved controls over ensuring VA claims are processed appropriately.

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

Rec. #1	***Finding***	Veteran Affairs Claim Review: 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.
	Recommendation	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.
	Status	As of August 14, 2019, OPM has collected $2,708,909, allowed $984,395 and there is a remaining receivable of $54,329,857. OPM also provided a memo dated September 12, 2019, with their position on the remaining questioned amount. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	$54,329,857
	Other Nonmonetary Benefit	N/A

Rec. #2	***Finding***	Veteran Affairs Claim Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a memo dated September 12, 2019, with their position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	Reduce future FEHBP payments over $20 million a year.
	Other Nonmonetary Benefit	Reduce veteran members' out-of-pocket expense by having lower cost shares.

Continued: Global Audit of Veterans Affairs for BCBS Plans		
Rec. #3	***Finding***	Veteran Affairs Claim Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a memo dated September 12, 2019, with their position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	Reduce future FEHBP payments over $20 million a year.
	Other Nonmonetary Benefit	Reduce veteran members’ out-of-pocket expense by having lower cost shares.
Rec. #4	***Finding***	Veteran Affairs Claim Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a memo dated September 12, 2019, with their position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	Reduce future FEHBP payments over $20 million a year.
	Other Nonmonetary Benefit	Reduce veteran members’ out-of-pocket expense by having lower cost shares

Continued: Global Audit of Veterans Affairs for BCBS Plans		
Rec. #5	***Finding***	Veteran Affairs Claim Review: 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.
	Recommendation	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.
	Status	OPM is still in the process of reviewing this recommendation and provided a memo dated September 12, 2019, with their position. We are currently in the process of reviewing this memo and will be preparing a response.
	Estimated Program Savings	Unknown – however, improving internal controls over how VA claims are processed and paid should result in increased program savings to health benefit charges, administrative cost, and member's cost share for health benefit services.
	Other Nonmonetary Benefit	Improved controls over ensuring VA claims are processed appropriately.

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.

Title: Audit of HMO Health Ohio **Report #: 1C-L4-00-16-013** **Date: September 23, 2016**		
Rec. #1	***Finding***	Defective Pricing: 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. 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.
	Recommendation	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 the [redacted]'s 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.
	Status	On August 29, 2019, OPM sent a resolution to the Plan requesting a proposed settlement to resolve this finding. OPM proposed a settlement of 50% of the total findings which equates to $1,588,904 for the defective pricing amounts. Upon receipt of the settlement amount, OPM would allow the remaining balance.
	Estimated Program Savings	$3,177,807
	Other Nonmonetary Benefit	To ensure that Federal employees and their employing agencies are paying a fair and reasonable price for health coverage.

Continued: Audit of HMO Health Ohio		
Rec. #2	***Finding***	Lost Investment Income: 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.
	Recommendation	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.
	Status	On August 29, 2019, OPM sent a resolution to the Plan requesting a proposed settlement to resolve this finding. OPM proposed a settlement of 50% of the total findings which equates to $261,666 for the lost investment income amount accrued through February 2019. Upon receipt of the settlement amount, OPM would allow the remaining balance.
	Estimated Program Savings	$523,331
	Other Nonmonetary Benefit	To ensure that the Federal Government receives reimbursement for interest lost on Program funds due to improper payments.

Title: Audit of Presbyterian Health Plan **Report #: 1C-P2-00-18-014** **Date: March 7, 2019**		
Rec. #2	***Finding***	Claims Paid for Capitated Members: The Plan paid unallowable Fee-for-Service (FFS) claims in 2015 for FEHBP members who were covered under an active capitation agreement. The erroneous payments are attributable to an apparent lack of internal controls over the coordination of capitation coverage and the payment of FFS claims.
	Recommendation	The OIG recommends that the OPM contracting officer verify that the Plan institute internal controls to identify fee-for-service claims paid for members who are actively enrolled and charged under a capitated arrangement.
	Status	Open and still under review.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	To ensure that the MLRs, reported by the Plan, are accurate. Also, to ensure that FEHBP members and their employing agencies are not paying for claims for members who are covered under a capitation agreement.

Continued: Audit of Presbyterian Health Plan

Rec. #5	***Finding***	Claims Paid for Ineligible Dependents: The Plan could not support the eligibility of two dependent members aged 26 and older in 2014 and 2015. As a result, the Plan paid $23,507 in medical and pharmacy claims for these members who may not be eligible for coverage.
	Recommendation	The OIG recommends that the OPM contracting officer verify that the Plan maintains supporting documentation for FEHBP dependents that have been designated as disabled.
	Status	Open and still under review.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	To ensure that the MLRs, reported by the Plan, are accurate. To ensure that FEHBP members and their employing agencies are paying for claims for members who are eligible for coverage.
Rec. #6	***Finding***	Claims Paid for Members after Effective Date of Termination: The Plan paid twelve medical claims totaling $3,952 in 2015 for four members after the effective date for termination of coverage. The Plan noted that while claims for one of the members were not adjusted, claims for the remaining three members were subsequently adjusted. However, the Plan did not provide support for these adjustments. Moreover, the adjustments occurred starting in August of 2016, and as such, would not have been reflected in the claims data used for the 2015 MLR calculation.
	Recommendation	The OIG recommends that the OPM contracting officer verify that the Plan enhance its internal controls over claims processing to ensure that claims are appropriately and timely adjusted when members' coverage is retroactively terminated.
	Status	Open and still under review.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	To ensure that the MLR's reported by the Plan are accurate. To ensure that FEHBP members and their employing agencies are paying for appropriate claims for the correct coverage period of the members.

V. 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.

Title: Management Alert – OPM's Procurement Process for Benefit Programs **Report #: 4A-RI-00-16-014** **Date: October 14, 2015**		
Rec. #2	***Finding***	Period of Performance Significantly Exceeded FAR Limits: 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.e.*, the Federal Employees Health Benefits Program and the Federal Employee Dental and Vision Insurance Program).
	Recommendation	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.
	Status	This recommendation was resolved, however it is still pending final action.
	Estimated Program Savings	Indirect savings - unknown
	Other Nonmonetary Benefit	Improved controls to ensure compliance with FAR and to enhance procurements integrity within OPM.

VI. EVALUATIONS

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

Title: Evaluation of OPM's Retirement Services' Customer Service Function
Report #: 4K-RS-00-16-023
Date: September 28, 2016

Rec. #1	***Finding***	Retirement Services is Not Providing Timely Responses to Annuitants' Inquiries – 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.
	Recommendation	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.
	Status	The agency partially agreed with this recommendation and is taking corrective action. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #2	***Finding***	Retirement Services is Not Providing Timely Responses to Annuitants' Inquiries – The OIG found that Retirement Services is not meeting its goal to respond to all written correspondence.
	Recommendation	The OIG recommends Retirement Services allocate additional resources to address the backlog of written correspondences.
	Status	The agency agreed with this recommendation and is taking corrective action. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Rec. #3	***Finding***	No Performance Measures to Assess Benefits of Imaging Efforts – 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.
	Recommendation	The OIG recommends that Retirement Services develop performance measures to determine if its imaging operations is achieving its intended results.
	Status	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.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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

Title: Evaluation Of The U.S. Office Of Personnel Management's Preservation of Electronic Records
Report #: 4K-CI-00-18-009

Date: December 21, 2018

Rec. #3	***Finding***	No Guidance on the Use of Smartphone Records Management for Official Government Business – OPM has not issued any specific guidance on the use of Government-issued smartphones, to include, restrictions on installing certain applications or procedures on the preservation of smartphone-generated records related to Government business.
	Recommendation	The OIG recommend that the Office of Chief Information Officer implement guidance on the official use of smartphones to include restrictions on usage and details on maintenance and preservation of records.
	Status	The agency agreed with this recommendation. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The OIG believes that by issuing formalized guidance on the use of government issued Smartphones decreases the risk of inadequate records management and increases compliance with Federal regulations related to the preservation of electronic records.

VII. MANAGEMENT ADVISORIES

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

Title: **Review of OPM's Non-Public Decision to Prospectively and Retroactively Re-Apportion Annuity Supplements** **Report #**: **L-2018-1** **Date**: **February 5, 2018**		
Rec. #1	***Finding***	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.
	Recommendation	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.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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.
Rec. #2	***Finding***	See number 1.
	Recommendation	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.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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		
Rec. #3	***Finding***	See number 1.
	Recommendation	The OIG recommends that OPM determine whether it has a legal requirement to make its updated guidance, including Retirement Insurance Letters, publicly available.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	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, 2019, 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	2	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
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-CF-00-15-027	FY 2015 Financial Statements	11/13/2015	5	5	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	4	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	2	0	$0
4A-CF-00-17-028	FY 2017 Financial Statements	11/13/2017	18	18	0	$0

Internal Audits Continued

Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4A-CF-00-15-049	OPM's Travel Card Program	01/16/2018	21	19	0	$0
4A-CF-00-16-055	OPM's Common Services	03/29/2018	5	5	0	$0
4A-CF-00-18-012	FY 2017 IPERA	5/10/2018	2	1	0	$0
4A-CF-00-18-024	FY 2018 Financial Statements	11/15/2018	23	23	0	$0
21	**Total Reports**		184	110	1	$108,880,417

Information Systems Audits

Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
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	2	0	$0
4A-CI-00-12-016	FISMA FY 2012	11/05/2012	18	3	0	$0
4A-CI-00-13-021	FISMA FY 2013	11/21/2013	16	4	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	14	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	2	0	$0
4A-CI-00-15-011	FISMA FY 2015	11/10/2015	27	15	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	20	0	$0

Information System Audits Continued

Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4A-RS-00-16-035	IT Sec. Controls OPM’s FACES	11/21/2016	13	2	0	$0
4A-CI-00-17-014	OPM’s Security Assessment & Authorization	06/20/2017	4	4	0	$0
4A-CF-00-17-044	OPM’s Federal Financial System	09/29/2017	9	2	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	36	0	$0
4A-CI-00-18-022	OPM's FY 2017 IT Modernization Expenditure	02/15/2018	4	4	0	$0
4A-HR-00-18-013	OPM’s USA Staffing System	05/10/2018	4	2	0	$0
4A-CI-00-18-044	OPM's FY 2018 IT Modernization Expenditure	06/20/2018	2	2	0	$0
4A-PP-00-18-011	OPM’s Health Claims Data Warehouse	06/25/2018	12	2	0	$0
4A-CI-00-18-038	FISMA FY 2018	10/30/2018	52	44	0	$0
IC-UX-00-18-019	Audit of Information Systems General and Application Controls at Medical Mutual of Ohio	1/24/2019	12	3	0	$0
25	**Total Reports**		415	184	0	$0

Claim Audits and Analytics

Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
1A-10-17-14-037	Health Care Service Corporation	11/19/2015	16	2	1	$24,721,545
lA-10-33-15-009	BCBS of North Carolina	11/10/2016	6	2	1	$17,652,501
1A-99-00-16-021	Global VA Claims for BCBS Plans	2/28/18	5	4	1	$54,329,857
3	**Total Reports**		27	8	3	$96,703,903

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	$3,701,138
1C-P2-00-18-014	Presbyterian Health Plan	03/07/2019	16	3	0	$0
1	**Total Reports**		18	3	2	$3,701,138

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
1	**Total Reports**		4	1	0	$0

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	1	0	$0
4K-CI-00-18-009	OPM's Preservation of Electronic Records	12/21/2018	3	1	0	$0
3	**Total Reports**		9	4	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	**Total Reports**		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