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

Open Recommendations

Open Recommendations Over Six Months Old as of September 30, 2020

November 30, 2020

EXECUTIVE SUMMARY

Open Recommendations Over Six Months Old as of September 30, 2020

November 30, 2020

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 VINT

Digitally signed by NORBERT VINT
DN: c=US, o=U.S. Government, ou=Office of Personnel Management, cn=NORBERT VINT, 0.9.2342.19200300.100.1.1=24001000006331
Date: 2020.11.25 11:11:08 -05'00'

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

As of September 30, 2020, there were 398 unimplemented recommendations, 208 of which are considered unique, 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 9/30/20	# Unique Recs. as of 9/30/20
Internal Audits	23	206	126	80
Information Systems Audits	27	480	254	110
Claim Audits and Analytics	2	22	2	2
Other Insurance Audits	1	5	3	3
Evaluations	4	16	11	11
Management Advisories	1	2	2	2
Total	**58**	**731**	**398**	**208**

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	125	1	$109 M
Information Systems Audits	254	0	$0
Claim Audits and Analytics	0	2	$1 M
Other Insurance Audits	3	0	0
Evaluations	11	0	0
Management Advisories	2	0	0
Total	**395**	**3**	**$110 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

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, 2020, 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, the independent public accountant employed by OPM to conduct the financial statement audit, 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, 2020, 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, 2020, 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.

* represents repeat recommendations.

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, 2020, 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, 2020, 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 has not yet received evidence that implementation has been completed.
	Estimated Program Savings	Potentially significant detection of and reduction in improper payments.
	Other Nonmonetary Benefit	Updated annuity roll records.

* represents repeat recommendations.

Continued: Stopping Improper Payments to Deceased Annuitants		
Rec. #2	***Finding***	Capitalizing on Retirement Systems Modernization (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. 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 detection of potential improper payments.

Title: Audit of the Fiscal Year 2011 Financial Statements **Report #: 4A-CF-00-11-050** **Date: November 14, 2011**		
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, 2020, 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: November 15, 2012**		
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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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 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, 2020, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2015 Financial Statements		
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, 2020, 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 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, 2020, 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. #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, 2020, 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 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 OPM's Office of Procurement Operations (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. #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.

Continued: Audit of OPM's Office of Procurement Operations' Contract Management Process		
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 OPO 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, 2020, 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, 2020, 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 Federal Information Security Management Act (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, 2020, 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, 2020, 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, the independent public accountant employed by OPM to conduct the financial statement audit, 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, 2020, 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, 2020, 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, 2020, 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], [redacted], and [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, 2020, 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, 2020, 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, 2020, 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, 2020, 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. #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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2016 Financial Statements		
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, 2020, 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 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 Annual Financial Report (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

* represents repeat recommendations.

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 information 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.

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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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.

* represents repeat recommendations.

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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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, 2020, 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. #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, 2020, 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.
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, 2020, 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.
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.

Continued: Audit of OPM's 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.
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.

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

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

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

Continued: Audit of OPM's Travel Card Program		
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 and is now resolved. Closure is contingent on the completion of corrective actions.
	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.

Continued: Audit of OPM's 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.
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 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.
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 the Improper Payments Elimination and Recovery Act (IPERA) and the Improper Payments Elimination and Recovery Improvement Act (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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements		
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, 2020, 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, 2020, 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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements		
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, 2020, 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. #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, 2020, 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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements		
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, 2020, 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. #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, 2020, 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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements		
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, 2020, 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.
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.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements		
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, 2020, 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.
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, 2020, 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. #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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements		
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, 2020, 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, 2020, 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. #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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2018 Financial Statements		
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, 2020, 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.

Title: Audit of the U.S. Office of Personnel Management's Fiscal Year 2018 Improper Payments Reporting **Report #: 4A-CF-00-19-012** **Date: June 3, 2019**		
Rec. #1	***Finding***	The Disability Earnings Match overpayments reported in the *Corrective Actions* section, on page 137, of the FY 2018 AFR is understated by $132,659.
	Recommendation	We recommend that Retirement Services strengthen their internal controls to ensure that the improper payments information is supported, reviewed, and validated prior to issuance to the OCFO.
	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 verify the calculations used in reporting improper payments amounts, improper payments will not be understated or overstated.

Continued: Audit of the U.S. Office of Personnel Management's Fiscal Year 2018 Improper Payments Reporting		
Rec. #3*	***Finding***	Beginning in FY 2015, the OIG reported that OPM was not properly categorizing the root causes of the retirement benefits program's improper payments in OPM's AFR. Retirement Services made improvements in FY 2016 by properly categorizing improper payments related to death data; however, they were 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.
	Recommendation	We recommend 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.
	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 OPM continues their efforts to provide transparency and granularity in the retirement benefits program's improper payments, they will better present the root causes of improper payments in the AFR.
Rec. #4*	***Finding***	In FY 2017, the OIG reported that while Retirement Services met its improper payments reduction targets, the overall intent of the Improper Payments Information Act of 2002, as amended by IPERA and IPERIA, to reduce improper payments, had not been met. In addition, we noted that Retirement Services outlined various corrective actions taken to combat improper payments; however, some had been discontinued due to the perceived cost ineffectiveness of the program, such as the Proof of Life project, and additional cost effective corrective actions have not been identified and implemented.
	Recommendation	We recommend 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 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 OPM develops and implements additional cost effective corrective actions, aimed at the root cause(s) of improper payments, they will further reduce the improper payments rate.

Title: Audit of the U.S. Office of Personnel Management's Oversight of the ID Experts Credit Monitoring and Identify Theft Services Contract **Report #: 4A- OO-00-18-006** **Date: October 11, 2019**		
Rec. #2	***Finding***	The COR did not perform all duties required by OPM's *Designation of Contracting Officer's Representative Form*. While reviewing the contract file and supporting documentation, we identified three instances of non-compliance.
	Recommendation	We recommend that OPM implement controls to ensure that the COR conducts site visits, when appropriate, to the contractor and subcontractor's facilities to review contractor performance. Controls should include maintenance of documentation showing the results of the site visits and/or rationale as to why site visits are not warranted.
	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	Not conducting site visits to the contractor and subcontractor's facilities to review contractor performance increases the chances that a contractor may not be performing work as required by the contract.
Rec. #3	***Finding***	See number 2 above.
	Recommendation	We recommend that OPM implement controls to ensure that the COR validates information included in the contractor's reports submitted to OPM. Controls should include maintenance of documentation supporting the COR's validation of the information, to include but not be limited to, the supporting documentation, exceptions, and follow-up questions with the contractor.
	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	Not validating the data received from the contractor increases the chances that a contractor may not be performing work as required by the contract.

Title: Audit of the U.S. Office of Personnel Management's Data Submission And Compliance With The Digital Accountability And Transparency Act Of 2014 **Report #: 4A-CF-00-19-025** **Date: November 6, 2019**		
Rec. #1	***Finding***	**System Linkage Discrepancies**- OPM needs to strengthen controls over its DATA Act submission process to ensure that no discrepancies exist in the linkages between Files C and D1.
	Recommendation	We recommend that the OCFO address system linkage discrepancies between Procurement Information System for Management (PRISM), Federal Procurement Data System-Next Generation (FPDS-NG), and Consolidated Business Information System (CBIS).
	Status	The agency agreed with the recommendation. The recommendation remains open pending the results of the upcoming FY 2021 DATA Act audit at which time we will determine if the recommendation can be closed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Addressing linkage discrepancies between PRISM, FPDS-NG, and CBIS will help to reduce publication of inaccuracies to USASpending.gov.
Rec. #2	***Finding***	**Internal Controls –**OCFO and OPO need to strengthen controls to ensure Files C and D1 are valid, accurate, and complete as required by OMB-17-04.
	Recommendation	We recommend that the OCFO work with OPO to strengthen controls to ensure Files C and D1 are valid, accurate, and complete as required by OMB-17-04. Controls at a minimum should include a review of Procurement Instrument Identifier Numbers, Transaction Obligation Amount, and Parent Award Identifier, and/or Data elements to ensure linkages across PRISM, FPDS-NG, and CBIS.
	Status	The agency agreed with the recommendation. The recommendation remains open pending the results of the upcoming FY 2021 DATA Act audit at which time we will determine if the recommendation can be closed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Valid, accurate, and complete documentation provided for Files C and D1 will help to reduce publication of inaccuracies to USASpending.gov.

Title: Audit of OPM's Fiscal Year 2019 Financial Statements **Report #: 4A-CF-00-19-022** **Date: November 18, 2019**		
Rec. #1*	***Finding***	**Security Access:** General Support Systems (GSSs) and application System Security Plans, Risk Assessments, Authority to Operate Packages and Information System Continuous Monitoring documentation were incomplete, not timely, or not reflective of current operating conditions.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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***	**Security Access:** 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 the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Enhance processes in place to track the inventory of OPM's systems and devices, and validate that security software and tools are installed on all systems.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
Rec. #3*	***Finding***	**Security Access:** 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 the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Implement a system or control that tracks the employment status of OPM contractors.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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.
Rec. #4*	***Finding***	**Security Access:** 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 the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
Rec. #5*	***Finding***	**Security Access:** 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 the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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***	**Logical Access:** Users, including those with privileged access, were not appropriately provisioned and de-provisioned access from OPM's information systems.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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. As of September 30, 2020, 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. #7*	***Finding***	**Logical Access:** OPM did not comply with their policies regarding the periodic recertification of the appropriateness of user access.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
Rec. #8*	***Finding***	**Logical Access:** 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 the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Implement two-factor authentication for applications.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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. #9*	***Finding***	**Logical Access:** System roles and associated responsibilities or functions, including the identification of incompatible role assignments, were not documented.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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 2019 Financial Statements		
Rec. #10*	***Finding***	**Logical Access:** Audit logging and monitoring procedures were not developed for all tools, operating systems, and databases contained within the application boundaries. Further, a comprehensive review of audit logs was not performed, or was not performed in a timely manner.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Prepare audit logging and monitoring procedures for databases within application boundaries. 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. As of September 30, 2020, 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. #11*	***Finding***	**Logical Access:** OPM could not provide a system generated listing of all users who have access to systems, as well as a listing of all users who had their access to systems revoked during the period.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Establish a means of documenting all users who have access to systems, and all users who had their systems access revoked.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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. #12*	***Finding***	**Logical Access:** Password and inactivity settings are not compliant with OPM policy.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Configure password and inactivity parameters to align with agency policies.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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 settings will ensure compliance with OPM policy.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
Rec. #13*	***Finding***	**Logical Access:** Memorandums of Understandings and Interconnection Service Agreements were not documented, signed, or reviewed on an annual basis.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Document, sign, and 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, 2020, 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 Memoranda of Understanding and Interconnection Service Agreements will increase the understanding of the contents and requirements of the agreements.
Rec. #14*	***Finding***	**Configuration Management:** 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 the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
Rec. #15	***Finding***	**Configuration Management:** Users have access to both, develop and migrate changes to the information systems. Additionally, there were instances in which OPM was unable to articulate users with access to develop and migrate changes to the information systems.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Separate users with the ability to develop and migrate changes to production, or implement controls to detect instances in which a user develops and migrates the same change.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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 to detect instances in which a user develops and migrates the same change decreases the risk that unauthorized users will have access to information systems.
Rec. #16	***Finding***	**Configuration Management:** OPM did not perform post-implementation reviews to validate that changes migrated to production were authorized for in scope systems.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Conduct post-implementation reviews to validate that changes migrated to production are authorized.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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	Conducting post-implementation reviews will ensure that changes migrated to production were authorized for in scope systems.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
Rec. #17*	***Finding***	**Configuration Management:** OPM did not maintain a security configuration checklist for platforms. Furthermore, baseline scans were not configured on all production servers within application boundaries. Lastly, misconfigurations identified through baseline scans were not remediated in a timely manner.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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. #18*	***Finding***	**Configuration Management:** Patch management procedures are outdated. Furthermore, patches were not applied in a timely manner.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Update patch management procedures to reflect current operating conditions. 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, 2020, 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	Updating patch management procedures will ensure that patches are applied in a timely manner and reflect current operating conditions..
Rec. #19*	***Finding***	**Interface / Data Transmission Controls:** Controls are not in place to validate that data transmitted to applications is complete and accurate.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Implement controls to validate that data transmitted to applications is complete and accurate.
	Status	The agency agreed with the recommendation. As of September 30, 2020, 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 data transmitted to applications is complete and accurate

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
Rec. #20*	***Finding***	**Interface / Data Transmission Controls:** Comprehensive interface / data transmission design documentation is not in place.
	Recommendation	Grant Thornton recommends that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: 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, 2020, 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	Develop interface / data transmission design documentation will ensure the completeness and accuracy of data transmitted, and definition of responsibilities.

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.

* represents repeat recommendations.

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.

* represents repeat recommendations.

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***	Systems development life cycle (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: 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.
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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2014		
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.
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 remediating vulnerabilities.

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

* represents repeat recommendations.

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

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2014		
Rec. #29	***Finding***	Contractor System Documentation: While the OCIO tracks ISAs, it does not track Memoranda 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 memoranda, 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.
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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2015		
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***	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 Memoranda 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 memoranda, 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.

* represents repeat recommendations.

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.

* represents repeat recommendations.

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.

* represents repeat recommendations.

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 National Institute of Standards and Technology (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.

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.

Continued: Audit of OPM's SharePoint Implementation		
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.
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.

Continued: Audit of OPM's SharePoint Implementation		
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.
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 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. #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.
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.

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

* represents repeat recommendations.

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

* represents repeat recommendations.

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

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

* represents repeat recommendations.

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

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

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

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

Continued: Federal Information Security Modernization Act Audit FY 2017		
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. #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.
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.

Continued: Audit of OPM's USA Staffing System		
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: 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.

* represents repeat recommendations.

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.

* represents repeat recommendations.

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	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.

* represents repeat recommendations.

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.

* represents repeat recommendations.

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 the U.S. Office of Personnel Management's Compliance with the Federal Information Technology Acquisition Reform Act **Report #: 4A-CI-00-18-037** **Date: April 25, 2019**		
Rec. #1	***Finding***	IT Budget Process: OPM has not maintained and enforced sufficient policies or procedures for ensuring the CIO's involvement in formulating its budgets. The OCIO is not routinely included in significant meetings and discussions around the core operating funds involving IT systems for other program offices.
	Recommendation	We recommend that the Office of the Director ensure that the CIO has adequate involvement and approval in all phases of annual and multi-year planning, programming, budgeting, and execution decisions in line with the Federal Information Technology Acquisition Reform Act (FITARA) and OMB Circular A-130 requirements.
	Status	OPM partially agreed with this recommendation and 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 appropriate approvals when formulating IT budgets.

Continued: Audit of the U.S. Office of Personnel Management's Compliance with the Federal Information Technology Acquisition Reform Act		
Rec. #2	***Finding***	Reprogramming of IT Funds: The CIO is not appropriately involved in the budget reprogramming process. There was no evidence to suggest there was CIO involvement in reprogramming decisions outside of those specific to the OCIO.
	Recommendation	We recommend that the Office of the Director ensure the CIO reviews and approves all reprogramming of funds for IT resources.
	Status	OPM partially agreed with this recommendation and 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 appropriate approval of IT fund reprogramming.
Rec. #3	***Finding***	Approval Process: The CIO does not officially approve all major project IT checklists as required by FITARA. The CIO delegates responsibility for approving IT checklists for major IT investments to the Deputy CIO.
	Recommendation	We recommend that the OCIO transition the responsibility for reviewing and approving checklists for major procurements to the CIO in accordance with FITARA.
	Status	OPM partially agreed with this recommendation and 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 appropriate approval of IT acquisitions.
Rec. #4	***Finding***	Approval Process: Procedures related to the IT checklists for non-major procurements as defined by FITARA and by OMB are not followed.
	Recommendation	We recommend that the OCIO update its procedures to only allow the CIO's direct reports to review and approve the IT checklists for non-major procurements as defined in FITARA and by OMB.
	Status	OPM partially agreed with this recommendation and 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 appropriate approval of non-major procurements.

Continued: Audit of the U.S. Office of Personnel Management's Compliance with the Federal Information Technology Acquisition Reform Act		
Rec. #5	***Finding***	IT Checklists: OPM's IT checklists have not been updated as required by OPM's policy. The Deputy CIO indicated that while the approval decisions were made based on accurate information, the lack of IT acquisition checklist revisions was an unintentional oversight.
	Recommendation	We recommend that the OCIO ensure that final approved checklists contain complete and accurate information.
	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 IT acquisitions are adequately tracked and any subsequent related IT acquisitions are correctly classified and approved.

Title: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration Data Warehouse **Report #: 4A-CI-00-19-006** **Date: June 17, 2019**		
Rec. #7	***Finding***	Contingency Plan Testing: The EHRIDW contingency plan test was conducted in April 2017, before the system migrated to OPM's Macon, Georgia data center. After the migration occurred and prior to the April 2018 Authorization, the Enterprise Human Resources Integration Data Warehouse (EHRIDW) did not conduct a contingency plan test.
	Recommendation	We recommend that OPM conduct a test of an updated EHRIDW contingency plan in accordance with the 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 recovering from an unplanned system outage.
Rec. #9	***Finding***	Role-Based Security Training: OPM requires all agency employees to complete annual security/privacy awareness training, however, this differs from role-based security training. Currently OPM does not provide role-based security training for EHRIDW personnel.
	Recommendation	We recommend that OPM provide and document role-based security training for the EHRIDW personnel with system level access.
	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 the Information Technology Controls of the U.S. Office of Personnel Management's Enterprise Human Resources Integration Data Warehouse		
Rec. #10	***Finding***	Audit Policies and Procedures: OPM has an agency-wide policy for Auditing and Accountability and procedures in place to enable the implementation of the policy for EHRIDW. However, OPM personnel involved in the auditing process were not aware of the procedures.
	Recommendation	We recommend that OPM disseminate auditing procedures to the individuals with auditing responsibilities and ensure the current process complies with the documented 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 ensuring that system auditing takes place.
Rec. #12	***Finding***	Policy and Procedures Providing Guidance for the Transition of a System's Management: OPM does not have any policies and procedures pertaining to the knowledge transfer required for a successful transition of a system's management between entities (e.g., from contractors to OPM employees, and conversely from OPM employees to contractors).
	Recommendation	We recommend that OPM develop policy and procedures to document requirements necessary for transitioning a system's management between entities.
	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 transition of a system's management.

Title: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Consolidated Business Information System **Report #: 4A-CF-00-19-026** **Date: October 3, 2019**		
Rec. #1	***Finding***	Control AT-3 – Role-Based Security Training: Currently, OPM does not provide or require role-based security training for CBIS personnel.
	Recommendation	We recommend that OPM provide and document role-based security training for CBIS personnel with system level access.
	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	Improved controls for managing information security risks at OPM.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Consolidated Business Information System		
Rec. #2	***Finding***	Control CM-6 – Configuration Settings: Baselines have not been defined by the agency. FAA previously scanned CBIS for Center for Internet Security standard compliance but switched to Defense Information Systems Agency standards without documenting approved settings nor allowed exceptions.
	Recommendation	We recommend that the OCFO work with FAA to implement standard security configuration settings for all operating platforms in use by CBIS.
	Status	The agency did not agree with the recommendation. Evidence to support their disagreement has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #3	***Finding***	Control IA-2(12) – Acceptance of PIV Credentials: The CBIS Application does not enforce Personal Identity Verification (PIV) authentication. Users currently log in via username and password.
	Recommendation	We recommend that the CBIS application meet the requirements of OMB M-11-11 by requiring 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. #4	***Finding***	Control IR-02 – Incident Response Training: OPM and FAA confirmed incident response training is not performed for CBIS despite the SSP stating that the control is inherited from FAA. FAA Information System Security Officers perform incident response training for other applications they support, but it is not performed for the CBIS application. Additionally, OPM system administrators do not perform incident response training specific to the CBIS application.
	Recommendation	We recommend that OPM ensure system administrators receive incident response training for CBIS.
	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	Improved controls for assessing and responding to security incidents.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Consolidated Business Information System		
Rec. #5	***Finding***	Control SA-22 – Unsupported Software Component: CBIS uses an unsupported software component, which is highly vulnerable. OPM has drafted a risk acceptance but it has not been approved. There is no timetable to upgrade the unsupported system component.
	Recommendation	We recommend that OPM maintain an approved risk acceptance for the unsupported software until the system is transitioned to a supported platform.
	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	Improved controls for ensuring up-to-date software.
Rec. #6	***Finding***	Control SA-22 – Unsupported Software Component: CBIS uses an unsupported software component, which is highly vulnerable. OPM has drafted a risk acceptance but it has not been approved. There is no timetable to upgrade the unsupported system component.
	Recommendation	We recommend that OPM remove or update the unsupported software from its environment.
	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	Improved controls for ensuring up-to-date software.
Rec. #7	***Finding***	Multi-factor Authentication to Datacenter: We performed a datacenter tour in June 2019 and found most physical and environmental controls mandated by NIST 800-53, Revision 4, to be in place. However, the FAA facility does not require multi-factor authentication to access the datacenter.
	Recommendation	We recommend that the OCFO ensure enforcement of multi-factor authentication at the CBIS datacenter for non-console access.
	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	Improved controls for access to sensitive areas.

Title: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative **Report #: 4A-CI-00-19-008** **Date: October 23, 2019**		
Rec. #2	***Finding***	Data Center Optimization - Automated Monitoring: Our FY 2018 FISMA Report included a series of recommendations to improve OPM's management of its systems, hardware, and software inventories. These recommendations remain open, and it is likely that the agency will have to address these FISMA recommendations before it can implement automated tools for infrastructure management.
	Recommendation	We recommend that OPM perform a gap analysis to identify the monitoring, inventory, and management tools that it needs to implement automated infrastructure management as required by the DCOI and OMB.
	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	Improved controls for identifying gaps in the agency's needs to implement automated infrastructure management
Rec. #3	***Finding***	Data Center Optimization - Power Metering: OPM does not have energy metering installed in all of its data centers.
	Recommendation	We recommend that OPM install automated power metering in all of its data centers in accordance with the requirements in the Data Center Optimization Initiative (DCOI).
	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	Improved controls to ensure a collection of information in order to produce a report on energy usage data in data centers.
Rec. #4	***Finding***	Reporting: OPM has complied with OMB's request, providing quarterly submissions. However, the submissions from Q1 FY 2017 through Q4 FY 2018 do not provide an accurate representation of OPM's data center inventory or DCOI compliance.
	Recommendation	We recommend that OPM assess the current state of its infrastructure to accurately report data center metrics, including the correct number of data centers (including non-tiered spaces), the correct operational status of data centers, and accurate energy usage.
	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	Improved controls for ensuring accurately report data center metrics.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative		
Rec. #5	***Finding***	Security Assessment and Authorization - LAN/WAN General Support System: OPM's current Authorization policies and procedures do not define requirements for addressing a change in authorizing official. Specifically, OPM's documentation does not require a new authorizing official to review system documentation and sign a new Authorization decision.
	Recommendation	We recommend that OPM update its Authorization policies and procedures to include requirements for reauthorizing systems in the event of a change in authorizing official. This guidance at a minimum should include parameters for the time period for re-authorization and requirements to evidence the system documentation reviews required by NIST.
	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	Improved controls for ensuring that current authorizing official agrees with information found in guidance.
Rec. #9	***Finding***	FIPS 199 Categorization - Macon General Support System: The Macon GSS is assessed as having a "moderate" impact level for each area, resulting in an overall categorization of "moderate." Our review of the system categorization from the prior Authorization noted that the document was not properly signed. Additionally, since the drafting of the Authorization, the Macon GSS now supports a major information system with a "high" categorization.
	Recommendation	We recommend that OPM categorize the Macon GSS as a high system and conduct a gap analysis to verify that the additional controls required for a high system are in place.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring appropriate system security categorization.
Rec. #10	***Finding***	Privacy Impact Assessment - ESI & LAN/WAN General Support Systems: In the most recent Authorizations, the ESI GSS's PTA was not complete (i.e., it did not indicate whether a PIA is required) or approved and the LAN/WAN GSS package did not include a PTA. PIAs for both GSSs were not provided during the course of the audit.
	Recommendation	We recommend that OPM complete and approve a PTA and PIA (if required by the PTA) for the ESI GSS in accordance with the requirements of the E-Government Act of 2002 and OPM policy.
	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	Improved controls for identifying privacy vulnerabilities existing on the information system.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative		
Rec. #11	***Finding***	Privacy Impact Assessment - ESI & LAN/WAN General Support Systems: In the most recent Authorizations, the ESI GSS's PTA was not complete (i.e., it did not indicate whether a PIA is required) or approved and the LAN/WAN GSS package did not include a PTA. PIAs for both GSSs were not provided during the course of the audit.
	Recommendation	We recommend that OPM complete and approve a PTA and PIA (if required by the PTA) for the LAN/WAN GSS in accordance with the requirements of the E-Government Act of 2002 and OPM policy.
	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	Improved controls for identifying privacy vulnerabilities existing on the information system.
Rec. #13	***Finding***	ESI General Support System: We reviewed the current ESI GSS SSP dated September 22, 2016, and determined that it does utilize the OPM template; however, the Chief Information Officer and Authorizing Official at the time of the Authorization in 2016 did not sign and approve the SSP. Additionally, we determined the SSP is incomplete. Specifically, there is a connection to the Sterling Forest backup site that is not sufficiently documented in the SSP.
	Recommendation	We recommend that OPM update and approve the ESI SSP to include all of the necessary information to fully document the Sterling Forest site.
	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	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. #14	***Finding***	Security Assessment Plan and Report - Macon General Support System: We identified one weakness in the control testing that was not subsequently included in the risk assessment and did not have a documented risk acceptance. There were 10 weaknesses evaluated in the risk assessment, 8 of which were mitigated, leaving only 2 open weaknesses. The two open weaknesses were appropriately added to the Macon GSS POA&Ms, however the weakness missing from the control assessment was not added.
	Recommendation	We recommend that OPM perform a gap analysis for the Macon GSS to assess the risk of the omitted control deficiency and update the POA&Ms to include all identified weaknesses.
	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	Improved controls for identifying gaps in Macon GSS controls and include those findings into POA&Ms.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative		
Rec. #15	***Finding***	Security Assessment Plan and Report - ESI General Support System: The assessment results table showed that there were 21 controls that were not fully satisfied. Additionally, there were eight controls that did not have a documented control assessment, and subsequently were not assessed for risk. Also, there were two weaknesses assessed for risk that were not appropriately included in the POA&Ms.
	Recommendation	We recommend that OPM perform a gap analysis for the ESI GSS to assess the risk of the omitted control deficiencies and update the POA&Ms to include all identified weaknesses.
	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	Improved controls for identifying gaps in ESI GSS controls and include those findings into POA&Ms.
Rec. #16	***Finding***	Contingency Plan - LAN/WAN General Support System: The current LAN/WAN GSS Contingency Plan is dated June 2014, and has not been updated on an annual basis as required. The contingency plan does not accurately reflect the current environment since the system infrastructure has undergone significant changes in the last five years (e.g., adding and removing data centers and systems).
	Recommendation	We recommend that OPM update and approve the contingency plan for the LAN/WAN GSS.
	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	Improved controls for recovering from an unplanned system outage.
Rec. #17	***Finding***	Contingency Plan Testing - LAN/WAN General Support System: OPM's LAN/WAN GSS contingency plan has not been updated in approximately five years and the LAN/WAN GSS environment has changed significantly in that time. Contingency plan testing is not effective when plans do not represent the current environment, system, and facilities.
	Recommendation	We recommend that OPM test the updated LAN/WAN contingency plan. This recommendation cannot be completed until Recommendation 16 has been implemented.
	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	Improved controls for recovering from an unplanned system outage.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative		
Rec. #18	***Finding***	Plan of Action and Milestones - Macon, ESI, & LAN/WAN General Support Systems: The Macon GSS, ESI GSS, and LAN/WAN GSS POA&Ms are generally documented according to OPM policy. However, OPM failed to adhere to remediation dates for its POA&M weaknesses.
	Recommendation	We recommend that OPM identify the necessary resources or process changes to ensure that POA&Ms are updated according to policy.
	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 agency is able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.
Rec. #19	***Finding***	Control PE-3(1) – Physical Access Control | Information System Access Macon, ESI, & LAN/WAN General Support Systems: The data centers in Macon, Georgia have an [redacted], but it is not in use by OPM.
	Recommendation	We recommend that OPM implement [redacted] at the data centers located in Macon, Georgia.
	Status	The agency did not agree with the recommendation. Evidence to support their disagreement has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for physical access the data center.
Rec. #20	***Finding***	Control PE-3(1) – Physical Access Control | Information System Access Macon, ESI, & LAN/WAN General Support Systems: The data centers in Washington, D.C. and Boyers, Pennsylvania have not implemented any [redacted]
	Recommendation	We recommend that OPM implement [redacted] at the data centers located in Washington, D.C.
	Status	The agency did not agree with the recommendation. Evidence to support their disagreement has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for physical access the data center.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative		
Rec. #21	***Finding***	Control PE-3(1) – Physical Access Control | Information System Access Macon, ESI, & LAN/WAN General Support Systems: The data centers in Washington, D.C. and Boyers, Pennsylvania have not implemented any [redacted]
	Recommendation	We recommend that OPM implement [redacted] at the data centers located in Boyers, Pennsylvania.
	Status	The agency did not agree with the recommendation. Evidence to support their disagreement has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for physical access the data center.
Rec. #23	***Finding***	Control PE-15 (1) – Water Damage Protection | Automation Support - ESI & LAN/WAN General Support Systems: During our tour of OPM's Washington, D.C. data centers, we did not identify water detection devices.
	Recommendation	We recommend that OPM implement automated water detection controls in the Washington, D.C. data centers.
	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	Decreases the risk of moisture/water damage to equipment.

Title: Federal Information Security Modernization Act Audit FY 2019 **Report #: 4A-CI-00-19-029** **Date: October 29, 2019**		
Rec. #1*	***Finding***	Inventory of Major Systems and System Interconnections: The current policy states that system owners are responsible for documenting system boundaries but a procedure for deciding what is or is not a part of a given system does not exist. The lack of a requirement to determine what is and is not part of a given system.
	Recommendation	We recommend that OPM improve the policies and procedures for defining system boundaries and classifying the systems in its environment.
	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	Improved controls for properly containing, sharing, and protecting sensitive information.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #2*	***Finding***	Inventory of Major Systems and System Interconnections: OPM struggles to identify and maintain the information about what resides in its environment.
	Recommendation	We recommend that the OCIO ensure that all interconnection security agreements are valid and properly maintained.
	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	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.
Rec. #3*	***Finding***	Inventory of Major Systems and System Interconnections: OPM struggles to identify and maintain the information about what resides in its environment.
	Recommendation	We recommend that the OCIO ensure that a valid memorandum of understanding/agreement exists for every interconnection.
	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	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.
Rec. #4	***Finding***	Hardware Inventory: Many assets are incomplete (e.g., missing serial numbers) or include inaccurate information (e.g., incorrect location). In addition, the hardware inventory does not contain information to associate hardware components to the major system(s) that they support.
	Recommendation	We recommend that OPM define the procedures for maintaining its hardware inventory.
	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	Improved controls for identifying and documenting systems and assets.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #5*	***Finding***	Hardware Inventory: Many assets are incomplete (e.g., missing serial numbers) or include inaccurate information (e.g., incorrect location). In addition, the hardware inventory does not contain information to associate 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	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	Improved controls for identifying and documenting systems and assets.
Rec. #6 *	***Finding***	Software Inventory: OPM has defined a policy requiring software components be inventoried in an agency centralized inventory.
	Recommendation	We recommend that OPM define policies and procedures for a centralized software inventory.
	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	Improved controls for understanding the information assets in the organization's environment.
Rec. #7*	***Finding***	Software Inventory: There was no information about where the software is located, how many copies exist, the responsible parties, or licensing. In addition, there were instances of unsupported software listed in the inventory.
	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	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	Improved controls for understanding the information assets in the organization's environment.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #8*	***Finding***	Software Inventory: The list of software only included application names and version numbers. There was no information about where the software is located, how many copies exist, the responsible parties, or licensing. In addition, there were instances of unsupported software listed in the inventory.
	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	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	Improved controls for identifying and remediating system vulnerabilities.
Rec. #9	***Finding***	Risk Policy and Strategy: OPM is not yet including supply chain risk management (SCRM) in its risk management processes. The agency's current risk profile, strategies, and policies do not specifically incorporate supply chain risks.
	Recommendation	We recommend that OPM develop an action plan and outline its processes to address the supply chain risk management requirements of NIST SP 800-161.
	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	Improved controls for addressing weaknesses in an appropriate timeframe and limiting system exposure to malicious attacks.
Rec. #10*	***Finding***	Information Security Architecture: OPM's enterprise architecture has not been updated since 2008 despite significant changes to its environment and plans, and does not support the necessary integration of an information security architecture. OPM has not documented an Information Security Architecture. In FY 2018, the agency contracted for enterprise architecture services, however, finalized architectures still do not exist.
	Recommendation	We recommend that OPM update its enterprise architecture, to include the information security architecture elements required by NIST and OMB guidance.
	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	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 2019		
Rec. #11*	***Finding***	Risk Management Roles, Responsibilities, and Resources: The agency has not been able to complete the annual requirement to test the security controls and contingency plans of all of its major information technology systems since 2008. OPM has not made sufficient progress in adopting a mature continuous monitoring program.
	Recommendation	We recommend that the OPM Director ensure that the OCIO has sufficient resources to adequately operate, secure, and modernize agency IT systems.
	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	Improved controls for managing information security.
Rec. #12*	***Finding***	Plan of Action and Milestones: OPM POA&M documentation has improved over prior years; however, we still noted the following issues as of August 2019 that 33 percent were more than 30 days overdue; 23 percent were more than 120 days overdue; and 45 percent are in draft or initial status (some since 2012).
	Recommendation	We recommend that OPM adhere to remediation dates for its POA&M weaknesses.
	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	Improved controls for managing POA&M weakness remediation.
Rec. #13*	***Finding***	Plan of Action and Milestones: OPM POA&M documentation has improved over prior years; however, we still noted the following issues as of August 2019 that 33 percent were more than 30 days overdue; 23 percent were more than 120 days overdue; and 45 percent are in draft or initial status (some since 2012).
	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 date should be maintained to track the schedule variance).
	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	Improved controls for managing POA&M weakness remediation.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #14	***Finding***	System Level Risk Assessments: Controls testing and risk assessments are a key part of the Authorization process, and the problems we found indicate that Authorizing Officials may not have all of the necessary risk information when granting an Authorization.
	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	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	Improved controls for conducting risk assessments.
Rec. #15*	***Finding***	Centralized Enterprise-wide Risk Tool: OPM does not have a system or tool to view centralized 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	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	Improved controls for capturing current enterprise risk information and assessing it in aggregate.
Rec. #16*	***Finding***	Risk Management Other Information - System Development Life Cycle: OPM last updated its System Development Life Cycle (SDLC) policy in 2013, and to date it is still not actively enforced for all IT projects.
	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	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	Improved controls for ensuring stability of systems development projects.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #17*	***Finding***	Configuration Management Roles, Responsibilities, and Resources: OPM has indicated that it does not have adequate resources (people, processes, and technology) to manage its Configuration Management (CM) program effectively.
	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	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	Improved controls for identifying gaps in the agency's configuration management program.
Rec. #18*	***Finding***	Configuration Management Plan: OPM has not established a process to document lessons learned from its change control process.
	Recommendation	We recommend that OPM document the lessons learned from its configuration management activities and update its configuration management plan as appropriate.
	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	Improved controls for analyzing and updating the agency's configuration management plan.
Rec. #19*	***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	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	Improved controls for ensuring that information systems are initially configured in a secure manner.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #20*	***Finding***	Baseline Configurations: OPM cannot currently run baseline configuration checks to verify that information systems are compliant 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 19 has been implemented.
	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	Improved controls for ensuring that servers are in compliance with approved security settings.
Rec. #21*	***Finding***	Security Configuration Settings: OPM has not implemented the process for exceptions, which means OPM did not customize the configuration settings for its systems and environment. As a result, testing against the Guides is not effective since OPM did not document the allowed deviations.
	Recommendation	We recommend that the OCIO develop and implement [standard security configuration settings] for all operating platforms in use by OPM.
	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	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #22*	***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 20 above has been completed.
	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	Improved controls for ensuring that servers are in compliance with approved security settings.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #23*	***Finding***	Security Configuration Settings: While OPM does utilize the Defense Information Systems Agency Security Technical Implementation Guides, OPM has not implemented the process for exceptions, which means OPM did not customize the configuration settings for its systems and environment.
	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	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	Improved controls for secure configuration of information systems.
Rec. #24*	***Finding***	Flaw Remediation and Patch Management: OPM is not routinely scanning every device on its network, 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 routine vulnerability scanning is conducted on all network devices documented within the inventory.
	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	Improved controls for identifying and remediating system vulnerabilities.
Rec. #25*	***Finding***	Flaw Remediation and Patch Management: OPM does not have a process to record or track the remediation status for other routine security 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	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	Improved controls for identifying and remediating system vulnerabilities.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #26*	***Finding***	Flaw Remediation and Patch Management: OPM is either not installing the patches in a timely manner or failing to document necessary exceptions to the patching policy.
	Recommendation	We recommend that the OCIO implement a process to apply operating system and third party vendor patches in a timely manner.
	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	Improved controls for identifying and remediating system vulnerabilities.
Rec. #27*	***Finding***	Flaw Remediation and Patch Management: OPM is not routinely scanning every device on its network, 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	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	Improved controls for identifying and remediating system vulnerabilities.
Rec. #28*	***Finding***	ICAM Roles, Responsibilities, and Resources: OPM does not consider ICAM to be a distinct program. In FY 2017, it was determined that OPM did not have a process in place to ensure that it provides adequate resources (people, processes, and technology) to stakeholders to fully implement ICAM controls. The agency took no corrective actions in FY 2018 or FY 2019.
	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	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	Improved controls for identifying the necessary resources required to maintain and progress OPM's ICAM program.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #29*	***Finding***	ICAM Strategy: In FY 2017, it was determined OPM has not developed and implemented an ICAM strategy containing milestones for how the agency plans to align with Federal ICAM initiatives. As noted above, OPM had not considered ICAM to be a distinct program and thus there were no corrective actions in FY 2018 or FY 2019.
	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	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	Improved controls for ensuring the success of the agency's ICAM initiatives.
Rec. #30*	***Finding***	Implementation of ICAM Program: In FY 2017, it was determined OPM has not developed and implemented an ICAM strategy containing milestones for how the agency plans to align with Federal ICAM initiatives. As noted above, OPM had not considered ICAM to be a distinct program and thus there were no corrective actions in FY 2018 or FY 2019.
	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	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	Improved controls for implementing the ICAM program with speed and efficiency.
Rec. #31*	***Finding***	Multi-factor Authentication with PIV: OPM has not configured multi-factor authentication for all major systems.
	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	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	Improved controls for implementing the ICAM program with speed and efficiency.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #32*	***Finding***	ICAM Other Information – Contractor Access Management: OPM does not centrally manage terminating contractor access. Furthermore, 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 timely removal of contractor accounts.
	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	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	Improved controls for preventing inappropriate access to critical or sensitive resources.
Rec. #33*	***Finding***	Data Protection and Privacy Policies and Procedures: OPM established the Chief Privacy Officer position and the Office of Privacy and Information Management (OPIM) in 2016 and 2019, respectively. Despite this substantial stride, OPM has not clearly defined the additional roles and responsibilities 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 disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for preventing data loss and mishandling of sensitive information.
Rec. #34*	***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, OPM has not updated this handbook since 2011, and it 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	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	Improved controls for preventing data loss and mishandling of sensitive information.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #35*	***Finding***	Data Breach Response Plan: OPM does not currently conduct routine 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	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	Improved controls for preventing major data loss in the event of a security incident.
Rec. #36*	***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	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	Improved controls for properly handling secure data and preventing data loss incidents.
Rec. #37*	***Finding***	Assessment of Workforce: OPM assessed the knowledge, skills, and abilities of its workforce as the first step to determine employees' specialized training needs. While OPM made progress in this area, a gap analysis, to determine any weaknesses and specialized training needs, must be performed.
	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	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	Improved controls for ensuring that OPM staff are fully prepared to address the security threats facing the agency.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #38*	***Finding***	ISCM Roles, Responsibilities, and Resources: The analysis identified and quantified the resource gap and confirms that the agency still does not have adequate resources to implement the activities effectively required by its ISCM strategy and policies.
	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 implement ISCM activities effectively based on OPM's policies and procedures.
	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	Improved controls for effectively implementing the agency's ISCM program, improving its ability to protect sensitive information.
Rec. #39*	***Finding***	Ongoing Security Assessments: We did observe that 6 of the 47 Authorizations provided were signed by an agency official who is no longer with OPM, a fact that necessitates re-authorization by the new authorizing official.
	Recommendation	We recommend that all active systems in OPM's inventory have a complete and current Authorization.
	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	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #40*	***Finding***	Ongoing Security Assessments: We did observe that 6 of the 47 Authorizations provided were signed by an agency official who is no longer with OPM, a fact that necessitates re-authorization by the new authorizing official.
	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.
	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	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #41*	***Finding***	Ongoing Security Assessments: We continue to find that many systems are not following the security control testing schedule that the OCIO mandated for all systems. For the first three quarters of FY 2019, OPM provided evidence of security control testing for 28 of OPM's 47 major systems. Of those, only eight systems were subject to security controls testing that complied with OPM's ISCM submission schedule for all three quarters.
	Recommendation	We recommend that OPM ensure that an annual test of security controls has been completed for all systems.
	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	Improved controls for implementing the agency's ISCM strategy and thereby reducing the risk of an attack.
Rec. #42	***Finding***	Measuring ISCM Program Effectiveness: OPM has not defined the format of reports measuring its ISCM program effectiveness.
	Recommendation	We recommend that OPM define a format for the reports used to communicate the effectiveness of its ISCM program.
	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	A clear and accurate report format will help give the reader an understanding about the effectiveness of ISCM program.
Rec. #43*	***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	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 41.
	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	Improved controls for ensuring proper security controls are in place.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #44*	***Finding***	Contingency Planning Roles and Responsibilities: Evidence shows that less than a quarter of the information systems have updated contingency plans and even less have performed contingency plan testing.
	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	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	Improved controls for being able to restore systems to an operational status in the event of a disaster.
Rec. #45*	***Finding***	Business Impact Analysis: OPM currently has a process in place to develop a Business Impact Analysis (BIA) at the information system level. Not all of OPM's major information systems have an approved BIA nor has this issue been identified in the POA&Ms.
	Recommendation	We recommend that the OCIO conduct an agency-wide BIA and incorporate the results into the system-level contingency plans. While OPM has performed an agency wide BIA, this recommendation remains open, as OPM has not incorporated the results into the system-level contingency plans.
	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	Improved controls for being able to restore systems based on criticality and therefore meet its recovery time objectives and mission.
Rec. #46*	***Finding***	Contingency Plan Maintenance: Only 7 of the 47 major systems have current contingency plans that were reviewed and updated in FY 2019. The OCIO needs to coordinate with the system owners and authorizing officials to ensure the contingency plans are in place and that an update occurs in accordance with policy. Currently, the OCIO is not sufficiently empowered to enforce the contingency planning policy.
	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	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	Improved controls for recovering from an unplanned system outage.

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #47*	***Finding***	Contingency Plan Testing: Only 5 of the 47 major information systems were subject to an adequate contingency plan test in FY 2019. Additionally, more than 60 percent of the 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	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	Improved controls for recovering from an unplanned system outage.

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[1] **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 August 3, 2020, OPM has collected $664,130 and allowed $33,629,597, leaving a remaining balance due of $1,269,235. OPM proposed a settlement requesting a return of $155,018 to close this recommendation. This amount is comprised of claims totaling $31,216 that were disallowed due to insufficient documentation and $123,802, which was a 10% projected amount due of the remaining overcharge ($1,269,235 - $31,216) based on OPM's review of other claims documentation.
	Estimated Program Savings	$1,933,365 ($664,130 + $1,269,235)
	Other Nonmonetary Benefit	N/A

[1] OPM OIG and the OPM Program Office have agreed to the closure of this recommendation. It is currently pending approval with the Acting Director.

Title: Audit of Claim Amounts Paid that Equaled or Exceeded Covered Charges at all Blue Cross and Blue Shield Plans[2] **Report #: 1A-99-00-18-005** **Date: March 13, 2020**		
Rec. #1	***Finding***	Claims Where Amounts Paid Equaled or Exceeded Covered Charges: Our review identified 396 improperly paid claims totaling $7,015,173 in net overcharges. This amount is comprised of $7,183,710 in overcharges ($7,183,940 - $230 immaterial adjustment) and $168,537 in undercharges. The identified overcharges stemmed from: • 290 claims paid incorrectly due to manual claim processor errors; • 58 claims paid incorrectly due to system errors; • 20 claims paid incorrectly due to provider billing errors; • 16 claims paid incorrectly due to untimely provider contract updates; • 2 claims that were not properly coordinated; and • 10 claims priced with an incorrect patient liability amount.
	Recommendation	We recommend that the contracting officer disallow $7,015,173 for claim overpayments and verify that the BCBS plans return all amounts recovered to the FEHBP.
	Status	Per an audit resolution letter dated August 11, 2020, $4,943,800 in overcharges has been recovered, $1,908,461 in overcharges has been allowed leaving a balance of $331,449 due to the Program. Once this amount has been returned to the Program, the undercharges of $168,537 will be allowed.
	Estimated Program Savings	$5,106,712
	Other Nonmonetary Benefit	N/A

[2] OPM OIG and the OPM Program Office have agreed to the closure of this recommendation. It is currently pending approval with the Acting Director.

IV. 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 Managers (PBMs) that that contract with and provide pharmacy benefits to carriers participating in the FEHBP.

Title: Audit of BENEFEDS as Administered by Long Term Care Partners, LLC[3] **Report #: 1G-LT-00-18-040** **Date: September 11, 2019**		
Rec. #1	***Finding***	Ineligible Dependents: Long Term Care Partners, LLC (LTCP) and OPM did not implement sufficient controls for BENEFEDS to ensure that only eligible dependents were enrolled in the Federal Employees Dental and Vision Insurance Program (FEDVIP). Specifically, we found that no controls were in place to stop ineligible family members from enrolling in the program, including ineligible grandchildren, multiple spouses, and families with a higher number of dependents per enrollee within the FEDVIP compared to the FEHBP. These dependent eligibility issues occurred, primarily, because OPM did not provide LTCP authority to request eligibility documentation at the time of enrollment within BENEFEDS. Additionally, LTCP did not implement all available and cost effective system edits for BENEFEDS that deter an enrollee from adding ineligible dependents, such as predominantly placing electronic certification language (e.g., insurance fraud warnings) upon enrollment and refining system edits that question enrollment anomalies (e.g., flagging multiple spouses). Instead, enrollees simply self-certify family members with no requirement for the FEDVIP carriers or BENEFEDS to verify dependent eligibility. This lack of responsibility by all parties involved increases the risk of fraud and abuse by not preventing ineligible dependents from enrolling in a Federal program that is funded entirely by Federal employees and annuitants. Because OPM and BENEFEDS have inadequate controls in place to verify dependent eligibility, the FEDVIP is vulnerable to ineligible family members enrolling in the program with increased costs being charged to Federal employees and annuitants.
	Recommendation	We recommend that the Contracting Officer require LTCP to include, separately and prominently, the following electronic certifications in the BENEFEDS enrollment portal for FEDVIP enrollees to acknowledge and accept: • A check box for the enrollee to acknowledge 18 USC § 1001 and the punishable offense for falsifying a Federal document. • A check box for the enrollee to acknowledge 18 USC § 1347 and the punishable offense for health care insurance fraud. • A check box explaining that the enrollee is responsible for providing proof of dependent eligibility to the FEDVIP carrier within 60 days of the request. • A check box for the enrollee to certify that their dependents are eligible for coverage in accordance with 5 USC § 8901 (5).
	Status	Resolved, milestones developed and full implementation by LTCP is in process.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.

[3] OPM OIG and the OPM Program Office have agreed to the closure of these recommendations. It is currently pending approval with the Acting Director.

Rec. #1 (Cont.)	***Other Nonmonetary Benefit***	Establishes controls to ensure ineligible dependents are deterred from enrolling in the FEDVIP and to enhance program integrity within OPM.

Continued: Audit of BENEFEDS as Administered by Long Term Care Partners, LLC		
Rec. #3	***Finding***	Ineligible Dependents: LTCP and OPM did not implement sufficient controls for BENEFEDS to ensure that only eligible dependents were enrolled in the FEDVIP. Specifically, we found that no controls were in place to stop ineligible family members from enrolling in the program, including ineligible grandchildren, multiple spouses, and families with a higher number of dependents per enrollee within the FEDVIP compared to the FEHBP. These dependent eligibility issues occurred, primarily, because OPM did not provide LTCP authority to request eligibility documentation at the time of enrollment within BENEFEDS. Additionally, LTCP did not implement all available and cost effective system edits for BENEFEDS that deter an enrollee from adding ineligible dependents, such as predominantly placing electronic certification language (e.g., insurance fraud warnings) upon enrollment and refining system edits that question enrollment anomalies (e.g., flagging multiple spouses). Instead, enrollees simply self-certify family members with no requirement for the FEDVIP carriers or BENEFEDS to verify dependent eligibility. This lack of responsibility by all parties involved increases the risk of fraud and abuse by not preventing ineligible dependents from enrolling in a Federal program that is funded entirely by Federal employees and annuitants. Because OPM and BENEFEDS have inadequate controls in place to verify dependent eligibility, the FEDVIP is vulnerable to ineligible family members enrolling in the program with increased costs being charged to Federal employees and annuitants.
	Recommendation	We recommend that the Contracting Officer: • Require BENEFEDS to adopt system edits that attempt to capture dependent enrollment anomalies that require an explanation, such as natural children with birthdates too close together (e.g., within one week to seven months), natural children with birthdates too far apart from their parents (e.g., 50 or more years apart), multiple spouses, multiple last names, and multiple addresses. • Provide BENEFEDS with the authority to request documentation in order to confirm eligibility for any questionable dependents that are identified with its system edits. • Require BENEFEDS and the FEDVIP carriers to share and maintain dependent eligibility documentation to ensure that all members are eligibile for coverage.
	Status	First bullet is resolved, milestones developed and full implementation by LTCP is in process. Second and third bullets are closed.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls to ensure ineligible dependents are identified in the FEDVIP and to enhance program integrity.

Continued: Audit of BENEFEDS as Administered by Long Term Care Partners, LLC		
Rec. #5	***Finding***	No Fraud and Abuse Program: LTCP does not have a vigorous fraud and abuse program that assesses vulnerabilities and detects and eliminates fraud and abuse, as required by the BENEFEDS solicitation. By not having a vigorous fraud and abuse, BENEFEDS enrollment and cash management functions are susceptible to fraud, waste, and abuse that can result in the loss of funds and increased premiums for Federal employees and annuitants.
	Recommendation	We recommend that LTCP work with the Contracting Officer to formally establish a vigorous fraud and abuse program that is similar to the fraud and abuse requirements of contractors in other OPM programs. Basic controls to help detect and eliminate fraud, waste, and abuse for BENEFEDS operations should include, but not be limited to: • Policies and procedures that address threats of internal and external fraud and abuse related to BENEFEDS; • Policies and procedures that require suspected instances of fraud, waste, and abuse (FWA) to be reported timely to the Contracting Officer and the respective carrier, when applicable; • Provision of annual FWA reports to the Contracting Officer; • Establishment of an FWA hotline that is accessible to internal and external stakeholders. In establishing such a hotline, the contractor should also establish a system for tracking all allegations received; • Implementation of BENEFEDS system edits that help reduce or eliminate fraudulent enrollments; • A compliance program that prohibits retaliation against whistleblowers; • A formal FWA awareness training, specific to BENEFEDS, that is required of all employees and subcontractors; and, • An FWA prevention, detection, investigation, and reporting manual, which should include all plans, policies, and procedures specifically involved in the BENEFEDS fraud and abuse program.
	Status	Resolved, milestones developed and full implementation by LTCP is in process.
	Estimated Program Savings	Indirect savings – unknown.
	Other Nonmonetary Benefit	Establishes controls to ensure FWA is minimized in the FEDVIP and to enhance program integrity.

V. EVALUATIONS

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

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.

Title: Evaluation of the U.S. Office Of Personnel Management's Employee Services' Senior Executive Service and Performance Management Office **Report #: 4K-ES-00-18-041** **Date: July 1, 2019**		
Rec. #1	***Finding***	Senior Executive Resources Services (SERS) management does not perform on-going monitoring or separate quality control reviews of QRB data.
	Recommendation	The OIG recommend that the Senior Executive Resources Services manager build on-going monitoring and quality control measures to ensure its staff complies with laws and regulations, reports complete and accurate data, and maintains adequate supporting documentation.
	Status	The agency partially 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 formalized procedures for on-going monitoring and quality control measures would provide reasonable assurance that staff complies with laws and regulations, reports complete and accurate data, and maintains adequate supporting documentation.
Rec. #2	***Finding***	Standard operating procedures does not: • Identify a key provision and requirements; • Specify what supporting documentation to maintain to indicate such; • Specify what documentation to maintain to support the review as a pre-Board verification; and • Contain an effective date. SERS management did not update the Qualifications Review Board's (QRB) Charter for panel members to remove requirements no longer in place. In addition, reference guides for agency customers does not • Include a key requirement; • Specify what supporting documentation must be provided by agencies to indicate such; and • Indicate what documentation must be provided by agency customers.
	Recommendation	The OIG recommend that the Senior Executive Resources Services manager update and finalize its standard operating procedures, the QRB Charter, and reference guides to ensure its staff and agency customers comply with laws and regulations.
	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 updating and finalizing standard operating procedures, the QRB Charter, and reference guides would provide reasonable assurance staff and agency customers comply with laws and regulations.

Continued: Evaluation of the U.S. Office Of Personnel Management's Employee Services' Senior Executive Service and Performance Management Office		
Rec. #3	***Finding***	Survey respondents indicated it would not hurt to revisit the current process and measurements as well as identify opportunities to improve the process: • Unclear if the process is evaluating (a) the skills of the candidate or the writing of the contractor, and (b) candidates fairly based on the experiences of the candidate; • The QRB process is too rigid and subjective and certification decisions are inconsistent; • More technology and some form of tracking packages through the QRB process to aid in responding to customer status inquiries; and • Training and Job Aid: Suggest posting the "Developing Your Executive Core Qualifications" webinar on the OPM website and send out the link.
	Recommendation	The OIG recommend that the Senior Executive Resources Services manager assemble a working group with appropriate stakeholders to collaborate, brainstorm, and develop ways to improve the process to include but not be limited to clearly defining terminology use and considering a more objective method for scoring, more technology, the compilation of QRB panel, and approaches to training.
	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 assembling a working group with appropriate stakeholders would rejuvenate the relationship with agency customers and improve the process.
Rec. #4	***Finding***	Based on the current standard operating procedures, there is no guidance for the Executive Resources and Performance Management manager to perform separate quality control measures of certified SES performance appraisal systems data.
	Recommendation	The OIG recommend that the Executive Resources and Performance Management manager develop and appropriately, document quality control measures to ensure its staff complies with laws and regulations, reports complete and accurate data, and maintains adequate supporting documentation.
	Status	The agency partially 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 formularized quality control measures would provide reasonable assurance that staff complies with laws and regulations, reports complete and accurate data, and maintains adequate supporting documentation.

Continued: Evaluation of the U.S. Office Of Personnel Management's Employee Services' Senior Executive Service and Performance Management Office		
Rec. #5	***Finding***	The standard operating procedures for processing SES, Senior Level, and Scientific and Professional certifications does not contain the current supervisor review practice; and The standard operating procedures for the staff does not include certain requirements identified in the Basic Senior Executive Service Performance Appraisal System Certification Process.
	Recommendation	The OIG recommend that the Executive Resources and Performance Management manager update its standard operating procedures to include supervisory review process explained and align with common practices for its activities, including maintaining support documentation.
	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 updating and finalizing standard operating procedures would provide reasonable assurance staff understands supervisory review process and activities including maintaining support documentation are align with common practices.

Title: Evaluation of the Presidential Rank Awards Program **Report #: 4K-ES-00-19-032** **Date: January 17, 2020**		
Rec. #1	***Finding***	Senior Executive Resources Services staff did not document verification of the nine percent statutory limit for the number of career Senior Executive Service and Senior-Level and Scientific and Professional nominees by agency. Sections 451.301 (c) and 451.302 (c) of Title 5 Code of Federal Regulations specify that each agency may nominate up to nine percent of its SES career appointees and up to nine percent of its senior career employees, respectively.
	Recommendation	The OIG recommend that the Senior Executive Resources Services manager Senior Executive Resources Services manager update and finalize its standard operating procedures to ensure its staff document required responsibilities.
	Status	Management concurred with this recommendation and stated that they will update and finalize their standard operating procedures to ensure staff document required responsibilities.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The OIG believes that updating and finalizing standard operating procedures would provide reasonable assurance staff documents require responsibilities.

Continued Evaluation of the Presidential Rank Awards Program		
Rec. #2	***Finding***	Standard operating procedures did not indicate how management performs on-going monitoring or separate quality control reviews to ensure compliance.
	Recommendation	The OIG recommend that the Senior Executive Resources Services management build on-going monitoring and quality control measures to ensure compliance.
	Status	Management concurred with this recommendation and indicated that they plan to build additional on-going monitoring and quality control measures to ensure compliance.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The OIG believes formularized quality control measures would provide reasonable assurance that staff complies with laws and regulations.
Rec. #3	***Finding***	Senior Executive Resources Services did not have controls in place for its staff to address processing interagency agreements with nominating agencies. During our evaluation, we identified open interagency agreements for prior years.
	Recommendation	The OIG recommend that the Senior Executive Resources Senior Executive Resources Services manager work with the appropriate offices to closeout interagency agreements from fiscal years 2016, 2017, and 2018.
	Status	Management concurred with this recommendation and stated that they will work with the Office of Chief Financial Officer and NBIB (now the Defense Counterintelligence and Security Agency within the Department of Defense) to closeout interagency agreements from FYs 2016, 2017, and 2018.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The OIG believes that appropriate controls would provide reasonable assurance staff close out interagency agreements before the end of the year award was provided.

Continued Evaluation of the Presidential Rank Awards Program		
Rec. #4	***Finding***	Standard operating procedures for the Senior Executive Resources Services staff did not include instructions on how to process the interagency agreement from nominating agencies for the NBIB on-site evaluation.
	Recommendation	The OIG recommend that the Senior Executive Resources Services manager update and finalize its standard operating procedures to include instructions for processing interagency agreement obligation forms for on-site evaluation. The standard operating procedures should include: • Instructions for initiating interagency agreement with nominating agencies, processing procedures, collecting payments, and de-obligating funds to ensure: o No work will commence and no costs will be incurred until the agreement is fully executed; o Agreed upon milestones are set each year to ensure agencies are promptly notified when final costs are known; and o Notify agencies promptly to close out agreements before the end of the calendar year. • Ongoing monitoring and quality control measures for the interagency agreements process.
	Status	Management concurred with this recommendation and indicated that they plan to work with the Office of Chief Financial Officer to define a more streamlined interagency agreement process moving forward and update and finalize its standard operating procedures to include instructions for the new process.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The OIG believes that updating and finalizing standard operating procedures would provide reasonable assurance staff close out interagency agreements.

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.

Title: Federal Employees Health Benefits Program Prescription Drug Benefit Costs **Report #: 1H-01-00-18-039** **Date: March 31, 2020 (Corrected); February 27, 2020 (Original)**		
Rec. #		
1	***Finding***	The OIG is concerned that OPM may not be obtaining the most cost effective pharmacy benefit arrangements in the FEHBP. As of 2019, the FEHBP and its enrollees spent over $13 billion annually on prescription drugs, comprising over 27 percent of the total cost of the program. The OIG feels strongly that OPM should take a more proactive approach to finding ways to curtail the prescription drug cost increases in the FEHBP. While the efforts made to date have undoubtedly helped control drug costs, we feel additional measures are needed to find more cost saving solutions to the problem of the growing costs of prescription drugs in the FEHBP.
	Recommendation	We recommend that OPM conduct a new, comprehensive study by seeking independent expert consultation on ways to lower prescription drug costs in the FEHBP, including but not limited to the possible cost saving options discussed in this report.
	Status	Open
	Estimated Program Savings	Unknown, potentially substantial.
	Other Nonmonetary Benefit	N/A
Rec. # 2	***Finding***	See number 1.
	Recommendation	We recommend that OPM evaluate any study conducted pursuant to recommendation 1 and, with due diligence, formulate recommendations and a plan for agency action based on the best interests of the government, the FEHBP, and its enrollees.
	Status	Open
	Estimated Program Savings	Unknown, potentially substantial.
	Other Nonmonetary Benefit	N/A

APPENDIX

Below is a chart listing all reports described in this document that, as of March 31, 2020, had open recommendations over six months old.

Internal Audits						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**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
4A-CF-00-15-027	FY 2015 Financial Statements	11/13/2015	5	4	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	3	1	$108,880,417
4A-CF-00-16-030	FY 2016 Financial Statements	11/14/2016	19	13	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	1	0	$0
4A-CF-00-17-028	FY 2017 Financial Statements	11/13/2017	18	17	0	$0
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	20	0	$0
4A-CF-00-19-012	FY 2018 IPERA	6/3/2019	4	3	0	$0

Internal Audits Continued						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**Monetary Findings**	
					# Open	**Amount**
4A-OO-00-18-006	OPM's Oversight of ID Experts Contract	10/11/2019	6	2	0	$0
4A-CF-00-19-025	OPM's Compliance with DATA Act	11/6/2019	2	2	0	$0
4A-CF-00-19-022	FY 2019 Financial Statements	11/18/2019	20	20	0	$0
23	**Total Reports**		206	125	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-00-14-016	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
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

Information System Audits Continued						
Report Number	**Name**	**Date**	**Total # of Findings**	**# of Open Procedural Findings**	**Monetary Findings**	
					# Open	**Amount**
4A-CF-00-17-044	OPM's Federal Financial System	09/29/2017	9	1	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	2	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-CI-00-18-038	FISMA FY 2018	10/30/2018	52	44	0	$0
4A-CI-00-18-037	FITARA	4/25/2019	5	5	0	$0
4A-CI-00-19-006	OPM's EHRIDW	6/17/2019	13	4	0	$0
4A-CF-00-19-026	OPM's CBIS	10/3/2019	7	7	0	$0
4A-CI-00-19-008	OPM's Compliance with Data Center Optimization	10/23/2019	23	17	0	$0
4A-CI-00-19-029	FISMA FY 2019	10/29/2019	47	47	0	$0
27	**Total Reports**		480	254	0	$0

Claim Audits and Analytics						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**Monetary Findings**	
					# Open	**Amount**
1A-10-17-14-037	Health Care Service Corporation	11/19/2015	16	0	1	$1,933,365
lA-99-00-18-005	Global APEG audit at all BCBS plans	3/13/2020	6	0	1	$162,912
2	**Total Reports**		22	0	2	$1,432,147

Other Insurance Audits						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**Monetary Findings**	
					# Open	**Amount**
1G-LT-00-18-040	BENEFEDS as Administered by LTCP	9/11/2019	5	3	0	$0
1	**Total Reports**		5	3	0	$0

Evaluations						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**Monetary Findings**	
					# Open	**Amount**
4K-RS-00-17-039	OPM's Retirement Services' Imaging Operations	3/14/2018	3	1	0	$0
4K-CI-00-18-009	OPM's Preservation of Electronic Records	12/21/2018	3	1	0	$0
4K-ES-00-18-041	OPM's Employee Services' Senior Executive Service and Performance Management Office	7/1/2019	6	5	0	$0
4K-ES-00-19-032	Presidential Rank Awards Program	1/17/2019	4	4	0	$0
3	**Total Reports**		16	11	0	$0

Management Advisories						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**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
1H-01-00-18-039	Federal Employees Health Benefits Program Prescription Drug Benefit Costs	3/31/2020 (Corrected); 2/27/2020 (Original)	2	2	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