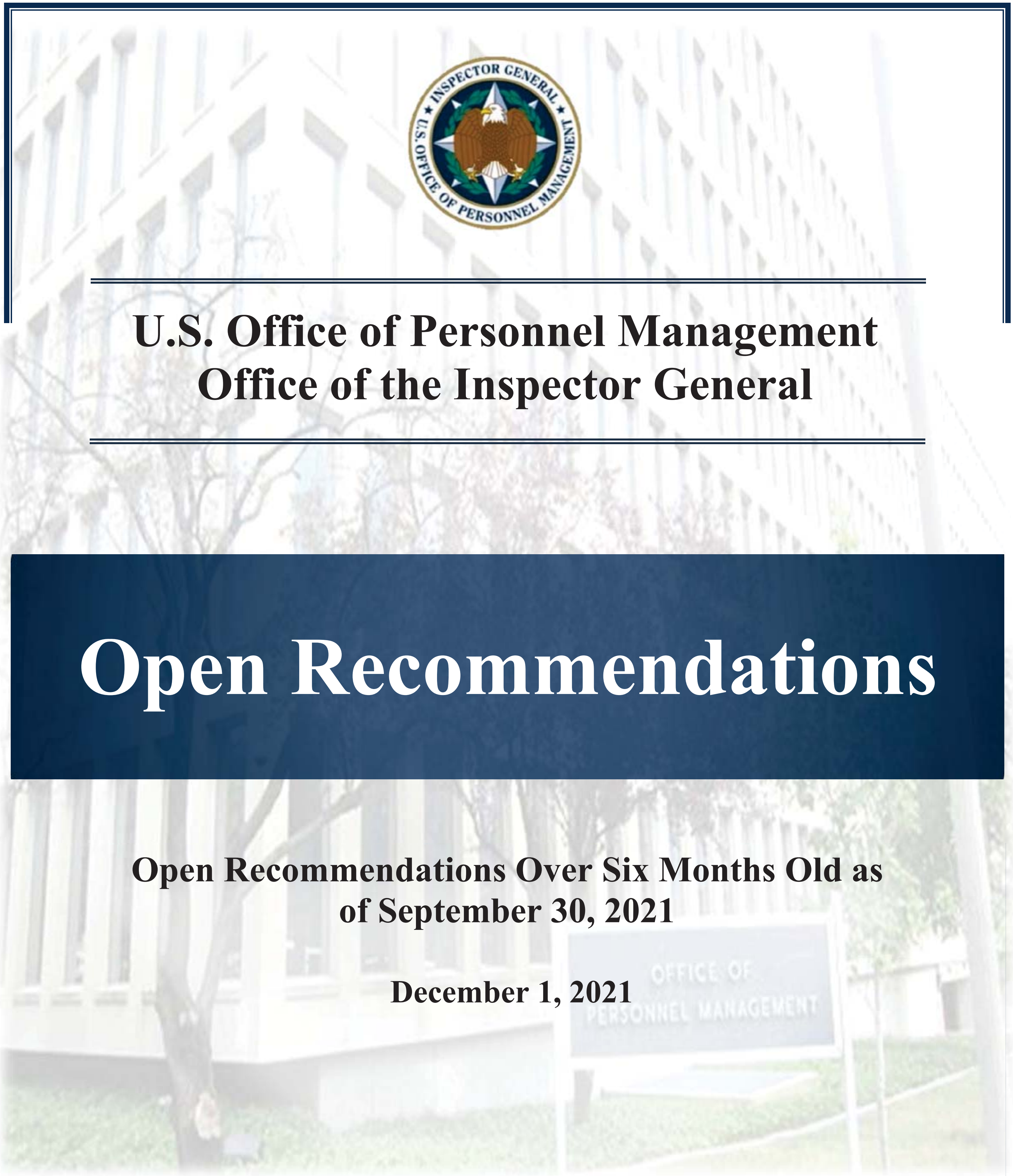

U.S. Office of Personnel Management
Office of the Inspector General

Open Recommendations

Open Recommendations Over Six Months Old as of September 30, 2021

December 1, 2021

Executive Summary

Open Recommendations Over Six Months Old as of September 30, 2021

December 1, 2021

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
Date: 2021.12.01 08:07:34 -05'00'

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

As of September 30, 2021, there were 396 unimplemented recommendations, 252 of which are considered unique, contained in reports that the OIG had issued to the U.S. Office of Personnel Management and over six months old.

Type of Report	# of Reports with Open Recs.	Total # Recs. Made	# Open Recs. as of 9/30/21	# Unique Recs. as of 9/30/21
Internal Audits	25	232	166	83
Information Systems Audits	39	637	191	116
Claim Audits and Analytics	3	4	4	4
Other Insurance Audits	2	32	18	18
Evaluations		16	10	10
Management Advisories and Other Reports	3	9	7	7
Total	**76**	**930**	**396**	**238**

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	165	1	$109 M
Information Systems Audits	191	0	$0
Claim Audits and Analytics	3	1	$1,227,289
Other Insurance Audits	17	1	$834,425
Evaluations	10	0	$0
Management Advisories and Other Reports	7	0	$0
Total	**393**	**3**	**$111 M**

**Totals are rounded.*

The term 'resolved' is used in some of the sections below. As defined in OMB Circular No. A-50, this means that the audit organization and agency management agree on action to be taken on reported findings and recommendations; however, corrective action has not yet been implemented. Outstanding and unimplemented (open) recommendations listed in this compendium that have not yet been resolved are not in compliance with the OMB Circular No. A-50 requirement that recommendations be resolved within six months after the issuance of a final report.

Abbreviations

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

Table of Contents

Page

Abbreviations.. ii

I. Internal Audits 1

II. Information Systems Audits...64

III. Claim Audits and Analytics 126

IV. Other Insurance Audits………………………………..............…………..…....129

V. Evaluations 136

VI. Management Advisories and Other Reports 141

Appendix: List of All Reports with Open Recommendations 151

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.[1]

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, 2021, 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.

[1] As defined in OMB Circular No. A-50, resolved means that the audit organization and agency management agree on action to be taken on reported findings and recommendations; however, corrective action has not yet been implemented. Outstanding and unimplemented (open) recommendations listed in this compendium that have not yet been resolved are not in compliance with the OMB Circular No. A-50 requirement that recommendations be resolved within six months after the issuance of a final report.

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 former 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, 2021, 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, 2021, 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, 2021, 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	OPM agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2021, 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 OPM 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 System Modernization 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, 2021, 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 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, 2021, 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, 2021, 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.

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, 2021, 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, 2021, 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 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, 2021, 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, 2021, 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, 2021, 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, 2021, 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. #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, 2021, 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 the Office of Procurement Operations' (OPO) contract files. In addition, OPO was unable to provide 17 of the 60 contract files, so we cannot determine if the amounts reported in CBIS were accurate.
	Recommendation	The OIG recommends that OPO implement internal controls to ensure that contract data, including contract award amounts, is accurately recorded in OPM's information systems, such as CBIS, and the appropriate supporting documentation is maintained.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are appropriately reported in OPM's financial management system.
Rec. #3	***Finding***	Weak Controls over the Contract Closeout Process - OPO could not provide a listing of contract closeouts for FY 2013 and FY 2014. In addition, of the 60 contracts the OIG sampled, we identified 46 in which OPO did not initiate the contract closeout process in compliance with the FAR.
	Recommendation	The OIG recommends that OPO develop an accurate inventory of FYs 2013 and 2014 contracts ready for closeout.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.
Rec. #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 Office of Procurement Operations return $108,880,417 in open obligations, for the 46 contracts questioned, to the program offices if support cannot be provided to show that the contract should remain open and the funds are still being utilized.
	Status	The agency agreed with the recommendation. OPM informed us that actions are in progress. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	$108,880,417
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.

Title: Audit of OPM's Fiscal Year 2016 Financial Statements **Report #: 4A-CF-00-16-030** **Date: November 14, 2016**		
Rec. #1	***Finding***	Information Systems Control Environment: The Information Security and Privacy Policy Handbook are outdated.
	Recommendation	Grant Thornton recommends that OPM review, update, and approve the security management policies and procedures at the organization defined frequency. Updates should incorporate current operational procedures and removal of outdated procedures and terminology.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2021, 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. • Risk Assessments – Conduct a risk assessment for financially relevant applications and systems and a document comprehensive results of the testing performed. • 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, 2021, 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 Modernization 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, 2021, 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, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	A listing of terminated contractors to be reconciled against systems access will decrease the risk that users retain lingering access to systems and therefore will decrease the risk of inaccurate, invalid, and unauthorized transactions being processed by systems that could ultimately impact financial reporting.
Rec. #5	***Finding***	Information Systems Control Environment: Role based training has not been completed.
	Recommendation	Grant Thornton recommends that OPM establish a means of documenting a list of users with significant information system responsibility to ensure the listing is complete and accurate and the appropriate training is completed.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2021, 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, 2021, 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. #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, 2021, 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 #9	***Finding***	Information Systems Control Environment: Physical Access to the Data Center is not Appropriately Restricted
	Recommendation	Grant Thornton recommends that OPM implement physical security controls over the datacenter so that users cannot gain unauthorized access and limit access to unauthorized individuals.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2021, 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. #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, 2021, 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 2016 Financial Statements		
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, 2021, 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***	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, 2021, 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 Federal Annuity Claims Expert System (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, 2021, 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 2016 Financial Statements		
Rec. #16	***Finding***	Information Systems Control Environment: OPM is unable to generate a complete and accurate listing of modifications to the mainframe and midrange environments.
	Recommendation	Grant Thornton recommends that OPM system owners establish a methodology to systematically track all configuration items that are migrated to production, and be able to produce a complete and accurate listing of all configuration items for both internal and external audit purposes, which will in turn support closer monitoring and management of the configuration management process.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Decreases the risk that unauthorized or erroneous changes to the mainframe and midrange configuration may be introduced without detection by system owners.
Rec. #17	***Finding***	Information Systems Control Environment: OPM lacks a security configuration checklist
	Recommendation	Grant Thornton recommends that OPM enforce existing policy requiring mandatory security configuration settings, developed by OPM or developed by vendors or federal agencies, are implemented and settings are validated on a periodic basis to ensure appropriateness.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2021, 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 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 Agency Financial Report (AFR), OPM acknowledges that they are aware of the major contributors of improper payments but are unable to provide the level of granularity needed to fully fulfill OMB Circular A-136 requirements. As a result, the remaining balance of these improper payments were placed in "Other Reason."
	Recommendation	The OIG recommends that OPM continue to implement controls to identify and evaluate the improper payment estimates root causes, to ensure that the root causes for the retirement benefits program's improper payments are properly categorized in OPM's annual AFR. (Rolled-Forward from FY 2015)
	Status	The agency did not agree with the recommendation. OPM is considering alternative approaches to address the findings. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place to identify the retirement services benefit programs improper payments estimates root cause, it will provide more granularity on the improper payment estimates, thus leading to more effective corrective actions at the program level and more focused strategies for reducing improper payments

Title: Audit of OPM's 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM’s Fiscal Year 2017 Financial Statements		
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, 2021, 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.
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, 2021, 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, 2021, 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, 2021, 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, 2021, 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. #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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2017 Financial Statements		
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, 2021, 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, 2021, 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. #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, 2021, 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 2017 Financial Statements		
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, 2021, 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, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	A thorough review of audit logs decreases the risk that suspicious activity that occurs may go undetected and therefore may not be addressed in a timely manner.
Rec. #15*	***Finding***	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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2017 Financial Statements		
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, 2021, 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM’s 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.
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.

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

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

Continued: Audit of OPM's Travel Card Program		
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.
Rec. #16	***Finding***	See #15 for description.
	Recommendation	The OIG recommends that Travel Operations implement stronger internal controls to ensure that travel card accounts are immediately cancelled upon separation of the cardholder's employment.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Cancelling cards immediately upon termination of employment decreases the opportunity for continued use, which can result in travel card misuse and abuse.
Rec. #17	***Finding***	We were unable to determine if inactive cardholder's accounts had been deactivated because documentation was not provided to show that periodic reviews of cardholder activity had been completed.
	Recommendation	The OIG recommends that Travel Operations identify cardholders that have not used their travel card for one year or more and deactivate travel cards in a timely manner.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.

Continued: Audit of OPM’s Travel Card Program		
Rec. #18	***Finding***	See #17 for description.
	Recommendation	The OIG recommends that Travel Operations enforce policies and procedures to conduct periodic reviews of travel card accounts to ensure cards are needed by the employees to which they are issued.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.
Rec. #19	***Finding***	See #17 for description.
	Recommendation	The OIG recommends that Travel Operations establish and implement controls to properly document and retain support for the periodic reviews of inactivity.
	Status	The agency agreed with the recommendation and it is now resolved. Closure is contingent on the completion of corrective actions.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Performing and documenting periodic review to identify travel cardholders that have not used their card decreases potential for misuse, abuse, and fraud.
Rec. #20	***Finding***	Travel Operations does not have controls in place to ensure that the travel card data reported in the Annual Financial Report is accurate.
	Recommendation	The OIG recommends that Travel Operations provide support to validate the travel card information provided in Table 18. Furthermore, we recommend Travel Operations improve internal controls over its travel card reporting process to ensure the integrity of the travel card data reported in the AFR. These controls should include verification and validation of the travel card information prior to reporting it in the AFR.
	Status	The agency agreed with the recommendation 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.

Continued: Audit of OPM's Common Services		
Rec. #2	***Finding***	See #1 for description
	Recommendation	The OIG recommends that the OCFO strengthen its internal controls to ensure that the distribution basis figures are properly supported, reviewed, and approved prior to billing the funding sources.
	Status	The agency agreed with the recommendation. OPM informed us that corrective actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If effective controls are in place to ensure errors are identified, funding sources will not be incorrectly charged for their share of common services.
Rec. #3	***Finding***	The OCFO could not produce documentation to support (1) that the Director approved the fiscal year 2017 common services cost of $105,101,530; (2) a change in Human Resources Solutions' common services January billing; and (3) how it determined the amount charged to the Office of the Inspector General.
	Recommendation	The OIG recommends that the OCFO provide documentation to support the Director's approval of the common services cost.
	Status	The agency agreed with the recommendation. OPM informed us that corrective actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Maintaining supporting documentation supports the common services cost and billing charges which help to ensure that OPM's funding sources have not been mischarged for common services.
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 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, 2021, 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.

* represents repeat recommendations.

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, 2021, 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, 2021, 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***	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, 2021, 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.

* represents repeat recommendations.

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, 2021, 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, 2021, 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, 2021, 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 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, 2021, 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, 2021, 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, 2021, 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.

* represents repeat recommendations.

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, 2021, 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, 2021, 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, 2021, 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, 2021, 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***	Memoranda of Understanding and Interconnection Service Agreements were not reviewed on an annual basis.
	Recommendation	Grant Thornton recommends that OPM review and update Interagency Service Agreements and Memoranda of Understanding in accordance with agency policies and procedures.
	Status	The agency agreed with the recommendation. As of September 30, 2021, 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. #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, 2021, 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.

* represents repeat recommendations.

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, 2021, 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, 2021, 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, 2021, 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.

* represents repeat recommendations.

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, 2021, 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***	Improper Payment Root Causes: 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.

* represents repeat recommendations.

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 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 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, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.

* represents repeat recommendations.

Rec. #1* (Cont.)	***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, 2021, 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***	**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, 2021, 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 2019 Financial Statements		
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, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The agency will be able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.
Rec. #5*	***Finding***	**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, 2021, 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
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, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Periodic reviews of personnel with access to systems will ensure the appropriateness of user access.
Rec. #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, 2021, 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, 2021, 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.

* represents repeat recommendations.

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, 2021, 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, 2021, 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, 2021, 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:** Memoranda of Understanding 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 Memoranda of Understanding in accordance with agency policies and procedures.
	Status	The agency agreed with the recommendation. As of September 30, 2021, 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, 2021, 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.

* represents repeat recommendations.

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, 2021, 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, 2021, 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, 2021, 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, 2021, 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, 2021, 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, 2021, 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.

Title: Audit of the U.S. Office of Personnel Management’s Federal Employees Health Benefits Program and Retirement Services Improper Payments Rate Methodologies
Report #: 4A-RS-00-18-035
Date: April 2, 2020

Rec. #1	***Finding***	Healthcare and Insurance’s (HI) FY 2017 reported improper payments rate methodology is outdated.
	Recommendation	We recommend that OPM’s Healthcare and Insurance office update its improper payments rate calculation, including a plan to do so with target dates, and documentation of any analysis conducted and conclusions reached in developing the updated methodology. This methodology, at a minimum, should include estimations for the population of the Federal Employees Health Benefits Program (FEHBP) carriers that have not been audited each year and statistically valid sampling to provide a more accurate representation of improper payments for reporting.
	Status	The agency partially 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	By updating its methodology, including considering the use of a statistically valid or alternative sampling and estimation approach to determine estimated improper payments for reporting purposes, the current methodology could be more in compliance with improper payments guidance and regulations. Moreover, OPM could more accurately report the amount of improper payments in a given FY.

* represents repeat recommendations.

Continued: Audit of the U.S. Office of Personnel Management's Federal Employees Health Benefits Program and Retirement Services Improper Payments Rate Methodologies		
Rec. #2	***Finding***	HI is only using the OIG's fraud data and recoveries to calculate its improper payments rate and is not including the fraud, waste, and abuse data from the FEHBP Fraud, Waste, and Abuse (FWA) Reports submitted by FEHBP carriers.
	Recommendation	We recommend that Healthcare and Insurance evaluate the data in the FWA Report to determine if the data can be simplified and validated, as necessary, to be used as a tool for its improper payments rate reporting.
	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	The FEHBP FWA Reports could be a valuable source of potential improper payment data, and the ability to verify and use the information means that HI could more accurately identify and report all of the FEHBP's improper payments.
Rec. #3	***Finding***	See number 2 above.
	Recommendation	We recommend that Healthcare and Insurance work with the FEHBP carriers to develop a process for reporting more uniform data in the FWA Report.
	Status	The agency partially 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	The FEHBP FWA Reports could be a valuable source of potential improper payment data, and the ability to verify and use the information means that HI could more accurately identify and report all of the FEHBP's improper payments.
Rec. #4	***Finding***	RS has not been utilizing the Do Not Pay (DNP) Portal. Since 2014, RS has reported their reasons for not using the DNP Portal in the AFR; however, the DNP Portal may be a control activity that RS could use to reduce improper payments.
	Recommendation	We recommend that Retirement Services continue to periodically meet with the DNP representatives to discuss new capabilities of the DNP Portal and determine whether it can be a beneficial addition in identifying improper payments for the most susceptible annuity payment cycle(s), i.e., pre-payment and post-payment.
	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	By taking steps to build a more robust improper payments methodology, RS could more accurately identify and report all of the FEHBP's improper payments.

Continued: Audit of the U.S. Office of Personnel Management's Federal Employees Health Benefits Program and Retirement Services Improper Payments Rate Methodologies		
Rec. #5	***Finding***	RS has not consistently conducted its Over Age 90 projects to verify the living status of the aged annuitant population and indicates that limited resources are impacting its ability to do so.
	Recommendation	We recommend that Retirement Services (RS) perform the Over Age 90 project of the annuitant population on a more routine basis, such as annually or biannually.
	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	The ability to perform the Over Age 90 projects on a more consistent basis has a clear impact on RS's ability to identify and stop annuity payments to ineligible annuitants and survivors.
Rec. #6	***Finding***	See number 5 above.
	Recommendation	We recommend that Retirement Services analyze the results from previous Over Age 90 projects to determine if the results can be projected to years where the Over Age 90 projects are not conducted and included in RS's improper payments reporting.
	Status	The agency partially 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	The ability to perform the Over Age 90 projects on a more consistent basis has a clear impact on RS's ability to identify and stop annuity payments to ineligible annuitants and survivors.
Rec. #7	***Finding***	See number 5 above.
	Recommendation	We recommend that all payments made to deceased annuitants be classified as improper in the year in which they are identified.
	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	By classifying payments as improper at the initial point of discovery, improper payments could be included in RS's calculation during the year in which they are identified.

* represents repeat recommendations.

Continued: Audit of the U.S. Office of Personnel Management's Federal Employees Health Benefits Program and Retirement Services Improper Payments Rate Methodologies		
Rec. #8	***Finding***	RS does not report overpayments identified during its annual Form 1099-R review in its improper payments rate calculation, including payments made to deceased annuitants where the reclamation process was initiated.
	Recommendation	We recommend that Retirement Services provide support to show the final results of the 9,169 cases in which reclamation was initiated and the 43 cases referred to the Survivor Processing Section from its review of returned 2016 tax year Form 1099-Rs.
	Status	The agency did not agree with the recommendation. The OIG has not received documentation to support their non-concurrence.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	By recognizing an improper payment as soon as an annuitant is identified as deceased and/or dropped from the annuity rolls, RS can ensure that the amount of improper payments is more accurately reported in the AFR.
Rec. #9	***Finding***	See number 8 above.
	Recommendation	We recommend that Retirement Services maintain support for future reviews of returned Form 1099-Rs, including an accounting of overpayments made to annuitants dropped from the annuity rolls, identified as deceased, or referred for further research and/or drop action, and include the total of such payments in the annual calculation of improper payments.
	Status	The agency partially 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	By recognizing an improper payment as soon as an annuitant is identified as deceased and/or dropped from the annuity rolls, RS can ensure that the amount of improper payments is more accurately reported in the AFR.
Rec. #10	***Finding***	RS did not provide any documentation on the nature of the underlying issues it experienced in conducting data mining reviews or its intent to address them.
	Recommendation	We recommend that Retirement Services conduct an analysis to determine if other types of data mining reviews can be performed, using the annuity roll data, to identify improper payments.
	Status	The agency partially agreed with the recommendation. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The increased use of data mining techniques could ensure that RS is not excluding a significant amount of improper payments from its improper payments rate calculation.

* represents repeat recommendations.

Continued: Audit of the U.S. Office of Personnel Management's Federal Employees Health Benefits Program and Retirement Services Improper Payments Rate Methodologies		
Rec. #11	***Finding***	See number 10 above.
	Recommendation	We recommend that Retirement Services develop a plan of action to utilize the data mining reviews identified in response to Recommendation 10 and report the results of those reviews in its improper payment calculation, including documenting any issues identified.
	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	The increased use of data mining techniques could ensure that RS is not excluding a significant amount of improper payments from its improper payments rate calculation.
Rec. #12	***Finding***	RS did not provide documentation to support that it completed any analysis of the cost effectiveness of their identified improper payment corrective actions, in accordance with OMB's Memorandum M-18-20, Circular A-123, Appendix C (Part III, A1), that would validate its position to discontinue activities, such as Proof of Life projects.
	Recommendation	We recommend that OPM's Retirement Services conduct cost benefit analyses of all current corrective actions and document their results.
	Status	The agency partially 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	The increased use of data mining techniques could ensure that RS is not excluding a significant amount of improper payments from its improper payments rate calculation.

Title: Audit of the U.S. Office of Personnel Management's Fiscal Year 2019 Improper Payments Reporting **Report #: 4A-CF-00-20-014** **Date: May 14, 2020**		
Rec. #1	***Finding***	Retirement Services and Healthcare and Insurance have not reviewed and updated their determination that a payment recapture audit program is not cost effective since 2011.
	Recommendation	We recommend that OPM conduct periodic analysis, based on current program conditions, on the cost-effectiveness of a payment recapture audit program and retain documentation to support their analysis and conclusion.
	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 OPM reviews and updates the analysis used to determine whether or not a payment recapture audit program is cost effective, it will ensure that OPM and the program offices are following guidance and best practices and potentially return improper payments to the trust funds.

Continued: Audit of the U.S. Office of Personnel Management's Fiscal Year 2019 Improper Payments Reporting		
Rec. #2*	***Finding***	Improper Payment Root Causes: 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 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.
Rec. #3*	***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, 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

* represents repeat recommendations.

Title: Audit of the U.S. Office of Personnel Management’s Retirement Services Disability Process
Report #: 4A-RS-00-19-038
Date October 30, 2020

Rec. #1	***Finding***	Retirement Services lacks the proper documentation, such as training certificates, sign-in sheets, or other supporting documentation, to verify that Boyers Disability Section, Appeals, and Claims I staff have completed the appropriate training to perform their job functions.
	Recommendation	We recommend that RS implement internal controls to ensure that all staff responsible for processing disability cases, including but not limited to Medical Specialists, Paralegals, and Legal Administrative Specialists, take the required training to perform their job functions and that supporting documentation for completed training is maintained.
	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 documenting Retirement Services’ staff’s training, it will increase OPM’s effectiveness in ensuring that disability cases are processed by qualified individuals.
Rec. #2	***Finding***	Retirement Services could not support that it met its requirement to annually reevaluate cases initially approved for disability retirement on a temporary basis until the annuitant reaches age 60, also known as Medical Call-ups.
	Recommendation	We recommend that RS establish a plan to complete the Medical Call-ups that are past the annual review period and stop any payments for which annuitants are no longer eligible.
	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 to ensure that Medical Call-ups are conducted timely, it will decrease OPM’s risk of not meeting requirements.
Rec. #3	***Finding***	See #2 for description.
	Recommendation	We recommend that RS ensure that Medical Call-ups are conducted timely and that supporting documentation is maintained.
	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 to ensure that Medical Call-ups are conducted timely, it will decrease OPM’s risk of not meeting requirements.

Continued: Audit of the U.S. Office of Personnel Management's Retirement Services Disability Process		
Rec. #4	***Finding***	See #2 for description.
	Recommendation	We recommend that RS investigate the cases due for Medical Call-ups in FY 2019 to determine if improper payments were made and immediately initiate any funds recovery, if applicable.
	Status	The agency partially 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 to ensure that Medical Call-ups are conducted timely, it will decrease OPM's risk of making improper payments.
Rec. #5	***Finding***	Claims I Quality Assurance Reviews were incomplete and not documented.
	Recommendation	We recommend that RS create and implement written procedures to ensure that quality assurance reviews are properly documented and maintained.
	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 to ensure that quality assurance reviews are documented, it will increase OPM's effectiveness in ensuring that quality assurance reviews are complete.
Rec. #6	***Finding***	See #5 for description.
	Recommendation	We recommend that RS ensure that Claims I/Claims II Internal Auditors and Senior LAS thoroughly complete quality assurance reviews for adjudicated cases.
	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	Ensuring that Retirement Services' staff thoroughly complete quality assurance reviews of adjudicated cases will increase RS' effectiveness over its claims process.

Continued: Audit of the U.S. Office of Personnel Management's Retirement Services Disability Process		
Rec. #7	***Finding***	We analyzed 61 out of 6,956 Retirement Disability Receipts for fiscal year 2019 and identified issues with processing timeliness and case tracking.
	Recommendation	We recommend that RS monitor internal timeliness goals to determine if they are practical and align with the updated disability process and new performance tracking systems, and modify the timeliness goals 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	Monitoring internal timeliness goals will increase Retirement Services' ability to ensure that disability cases are being properly tracked.
Rec. #8	***Finding***	See #7 for description.
	Recommendation	We recommend that Retirement Services continue to work with OPM's Office of the Chief Information Officer to establish a modernized Information Technology system that has capabilities to ensure the proper tracking of cases throughout the disability process.
	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	Modernizing OPM's information technology systems will enable Retirement Services to properly track its disability cases.

* represents repeat recommendations.

Title: Audit of OPM's Fiscal Year 2020 Financial Statements
Report #: 4A-CF-00-20-024
Date November 13, 2020

Rec. #1*	***Finding***	**Security Management:** 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	We recommend 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, 2021, 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 Management:** 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	We recommend 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
Rec. #3*	***Finding***	**Security Management:** 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	We recommend 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 current and separated OPM contractors.
	Status	The agency agreed with the recommendation. As of September 30, 2021, 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 Management:** 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	We recommend 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, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The agency will be able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.
Rec. #5*	***Finding***	**Security Management:** 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	We recommend 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
Rec. #6	***Finding***	**Security Management:** OPM did not review applicable Service Organization Controls (SOC) reports.
	Recommendation	We recommend that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to: Assign individuals the responsibility of reviewing SOC reports for systems that are leveraged by the agency and hosted and / or maintained by third parties.
	Status	The agency agreed with the recommendation. As of September 30, 2021, 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	Without a review the report of the controls performed by third parties, OPM is unable to validate that the internal control environment can mitigate risks.
Rec. #7*	***Finding***	**Logical Access:** Users, including those with privileged access, were not appropriately provisioned and de-provisioned access from OPM's information systems.
	Recommendation	We recommend 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, 2021, 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***	**Logical Access:** OPM did not comply with their policies regarding the periodic recertification of the appropriateness of user access.
	Recommendation	We recommend 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, 2021, 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 2020 Financial Statements		
Rec. #9*	***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	We recommend 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, 2021, 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. #10*	***Finding***	**Logical Access:** System roles and associated responsibilities or functions, including the identification of incompatible role assignments, were not documented.
	Recommendation	We recommend 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
Rec. #11*	***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	We recommend 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, 2021, 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. #12*	***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	We recommend 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, 2021, 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***	**Logical Access:** Password and inactivity settings are not compliant with OPM policy.
	Recommendation	We recommend 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, 2021, 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 2020 Financial Statements		
Rec. #14*	***Finding***	**Logical Access:** Memorandums of Understandings (MOUs) and Interconnection Service Agreements (ISAs) were not documented, signed, or reviewed on an annual basis.
	Recommendation	We recommend 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, 2021, 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. #15*	***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	We recommend 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
Rec. #16*	***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	We recommend 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, 2021, 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. #17*	***Finding***	**Configuration Management:** OPM did not perform post-implementation reviews to validate that changes migrated to production were authorized for in scope systems.
	Recommendation	We recommend 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, 2021, 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.

* represents repeat recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
Rec. #18*	***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	We recommend 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, 2021, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Restrictive security settings in place for components and a periodic assessment to ensure that such settings are in place and appropriate decreases the risk that the confidentiality, integrity, and / or availability of financial data is compromised.
Rec. #19*	***Finding***	**Configuration Management:** Patch management procedures are outdated. Furthermore, patches were not applied in a timely manner.
	Recommendation	We recommend 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, 2021, 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. #20*	***Finding***	**Interface/Data Transmission Controls:** Controls were not in place to validate that data transmitted to applications is complete and accurate.
	Recommendation	We recommend 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, 2021, 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 2020 Financial Statements		
Rec. #21*	***Finding***	**Interface/Data Transmission Controls:** Comprehensive interface / data transmission design documentation is not in place.
	Recommendation	We recommend 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, 2021, 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.[2]

Title: Federal Information Security Management Act Audit FY 2008 **Report #: 4A-CI-00-08-022** **Date: September 23, 2008**		
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. #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.

[2] As defined in OMB Circular No. A-50, resolved means that the audit organization and agency management agree on action to be taken on reported findings and recommendations; however, corrective action has not yet been implemented. Outstanding and unimplemented (open) recommendations listed in this compendium that have not yet been resolved are not in compliance with the OMB Circular No. A-50 requirement that recommendations be resolved within six months after the issuance of a final report.

Title: Federal Information Security Management Act Audit FY 2010
Report #: 4A-CI-00-10-019
Date: November 10, 2010

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. #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.

* represents repeat recommendations.

Title: Federal Information Security Management Act Audit FY 2012 **Report #: 4A-CI-00-12-016** **Date: November 5, 2012**		
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. #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. #7	***Finding***	Configuration Management: However, several additional operating platforms in OPM's network environment do not have baseline configurations documented.
	Recommendation	We recommend that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2014		
Rec. #7 (Cont.)	***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. #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.

Title: Audit of Information Security Controls of the U.S. Office of Personnel Management's Annuitant Health Benefits Open Season System **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 the Annuitant Health Benefits Open Season System (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.

* represents repeat recommendations.

Continued: Audit of Information Security Controls of the U.S. Office of Personnel Management's Annuitant Health Benefits Open Season System		
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 [redacted]
	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 [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 physical access to the data center.

Title: Federal Information Security Management Act Audit FY 2015 **Report #: 4A-CI-00-15-011** **Date: November 10, 2015**		
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]
	Status	OPM is taking corrective 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***	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2015		
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.

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.
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.

* represents repeat recommendations.

Continued: Audit of OPM’s Web Application Security Review

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. #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.

* represents repeat recommendations.

Continued: ***Federal Information Security Management Act Audit FY 2016***		
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]
	Status	OPM is taking corrective 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.
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.

* represents repeat recommendations.

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 the Information Systems General and Application Controls at UnitedHealthcare **Report #: 1C-JP-00-16-032** **Date: January 24, 2017**		
Rec. #2	***Finding***	Configuration Management: The results of our vulnerability and compliance scans indicate that several servers contain insecure configurations. We also detected isolated instances of servers that were not in compliance with established configuration baselines.
	Recommendation	We recommend that (UnitedHealthcare) UHC remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scanning audit inquiry provided directly to UHC.
	Status	This recommendation is resolved. UnitedHealthcare is taking corrective 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.

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 (SSP): The LAN/WAN SSP does not fully and accurately identify all of the security controls applicable to this system.
	Recommendation	We recommend 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.

* represents repeat recommendations.

Continued: Audit of OPM's Security Assessment and Authorization		
Rec. #2	***Finding***	System Controls Assessment: The local area network/wide area network (LAN/WAN) security controls assessment likely did not identify vulnerabilities that could have been detected with a thorough test.
	Recommendation	We recommend 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. #4	***Finding***	Other Authorization Packages: Many of the Authorization packages completed as part of the Sprint were not complete.
	Recommendation	We recommend 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 the Information Systems General and Application Controls at MVP Health Care **Report #: 1C-GA-00-17-010** **Date: June 30, 2017**		
Rec. #8	***Finding***	System Lifecycle Management: MPV Healthcare's (MVP)s computer server inventory indicates that numerous servers are running unsupported versions of operating systems. Software vendors typically announce projected dates for when they will no longer provide support or distribute security patches for their products (known as end-of-life dates). In order to avoid the risk associated with operating unsupported software, organizations must have a methodology in place to phase out software before it reaches its end-of-life date.
	Recommendation	We recommend that MVP update and/or enforce its system lifecycle methodology to ensure that information systems are [redacted]
	Status	This recommendation is resolved. MVP is taking corrective 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.

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

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.

* represents repeat recommendations.

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

Rec. #7	***Finding***	Software Inventory: OPM's software inventory does not contain the level of detail necessary for thorough tracking and reporting.
	Recommendation	The OIG recommends that OPM define the standard data elements for an inventory of software assets and licenses with the detailed information necessary for tracking and reporting, and that it update its software inventory to include these standard data elements.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for understanding the information assets in the organization's environment.
Rec. #9	***Finding***	Information Security Architecture: OPM's enterprise architecture has not been updated since 2008, and it does not support the necessary integration of an information security architecture.
	Recommendation	The OIG recommends that OPM update its enterprise architecture to include the information security architecture elements required by NIST and OMB guidance.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for aligning the agency's security processes, systems, and personnel with the agency mission and strategic plan.
Rec. #11*	***Finding***	Plan of Action and Milestones: Over 96 percent of POA&Ms were more than 30 days overdue and over 88 percent were more than 120 days overdue.
	Recommendation	The OIG recommends that OPM adhere to remediation dates for its POA&M weaknesses.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing POA&M weakness remediation.
Rec. #12	***Finding***	Plan of Action and Milestones: Over 96 percent of POA&Ms were more than 30 days overdue and over 88 percent were more than 120 days overdue.
	Recommendation	The OIG recommends that OPM update its POA&M entries to reflect both the original and updated remediation deadlines when the control weakness has not been addressed by the originally scheduled deadline (i.e., the POA&M deadline should not reflect a date in the past).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing POA&M weakness remediation.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2017		
Rec. #13	***Finding***	System Level Risk Assessments: A majority of risk assessments for systems that were authorized in FY 2017 had issues with the security control testing and/or the corresponding risk assessment.
	Recommendation	The OIG recommends that OPM complete risk assessments for each major information system that are compliant with NIST guidelines and OPM policy. The results of a complete and comprehensive test of security controls should be incorporated into each risk assessment.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for conducting risk assessments.
Rec. #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. #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. #22*	***Finding***	Security Configuration Setting Deviations: OPM has not tailored and documented any potential business-required deviations from the configuration standards.
	Recommendation	For OPM configuration standards that are based on a pre-existing generic standard, the OIG recommends that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for secure configuration of information systems.
Rec. #28	***Finding***	ICAM Strategy: OPM has not developed an Identity, Credential, and Access Management (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. #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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2017		
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.

* represents repeat recommendations.

Continued: OPM's FY 2017 IT Modernization Expenditure Plan		
Rec. #4	***Finding***	Modernization Strategy: The OIG believes that OPM’s business units continue to have an improper level of influence over IT management, and that the CIO’s office does not directly receive the dedicated funding needed to fulfill its mission.
	Recommendation	The OIG recommends that the OPM Director ensure that the CIO has the appropriate level of control over the IT acquisition and budgeting process across all of OPM.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for establishing the proper resources needed for the planning and execution of a successful IT modernization strategy.

Title: Audit of OPM’s USA Staffing System **Report #: 4A-HR-00-18-013** **Date: May 10, 2018**		
Rec. #3	***Finding***	Unapproved Configuration Deviations: Configuration deviations for the USA Staffing System have not been documented and approved.
	Recommendation	We recommend that OPM apply the approved security configuration settings for the USA Staffing System.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for reducing system weaknesses.
Rec. #4	***Finding***	Missing Patches: Several of the USA Staffing System servers were missing patches more than 30 days old.
	Recommendation	We recommend that OPM apply system patches in a timely manner and in accordance with policy.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for reducing system weaknesses.

Title: Audit of the Information Systems General and Application Controls at Optima Health Plan
Report #: 1C-PG-00-17-045
Date: May 10, 2018

Rec. #11	***Finding***	Removable Media: Sentara and Optima user endpoint devices are configured to enforce encryption on all data copied to removable media. [redacted]
	Recommendation	We recommend that Sentara restrict the use of removable media on users' workstations to those with a valid and approved business need.
	Status	This recommendation is resolved. Optima is taking corrective 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.

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. #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.
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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2018		
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 National Institute of Standards and Technology (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. #19*	***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	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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2018		
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.
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. #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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2018		
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. #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. #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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2018		
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.
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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2018		
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.
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.

* represents repeat recommendations.

Title: Audit of the Information Systems General and Application Controls at Medical Mutual of Ohio Report #: 1C-UX-00-18-019 Date: January 24, 2019		
Rec. #5	*Finding*	Network Access Controls: Medical Mutual [redacted]
	Recommendation	We recommend that Medical Mutual implement [redacted]
	Status	This recommendation is resolved. Medical Mutual is taking corrective 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.

Title: Audit of the Information Systems General and Application Controls at UPMC Health Plan Report # 1C-8W-00-18-036: Date: March 1, 2019		
Rec. #1	*Finding*	Internal Network Segmentation: No [redacted]
	Recommendation	We recommend that UPMC Health Plan [redacted]
	Status	This recommendation is resolved. UPMC is taking corrective 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.

Title: Audit of the Information Systems General and Application Controls at Priority Health Plan Report #: 1C-LE-00-18-034 Date: March 5, 2019		
Rec. #2	*Finding*	Internal Network Segmentation: [redacted]
	Recommendation	[redacted]
	Status	This recommendation is resolved. Priority Health is taking corrective 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.

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.
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.

Continued: Audit of the U.S. Office of Personnel Management's Compliance with the Federal Information Technology Acquisition Reform Act

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.
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.

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 Systems General and Application Controls at Kaiser Foundation Health Plan, Inc., Northern and Southern California Regions **Report #: 1C-59-00-19-005** **Date: July 23, 2019**		
Rec. #1	***Finding***	Internal Network Segmentation: However, there is limited [redacted] Kaiser of CA previously identified this as an area for improvement and has a project in progress to remediate the weakness.
	Recommendation	We recommend that Kaiser of CA complete its current project for the implementation of additional [redacted]
	Status	This recommendation is resolved. Kaiser is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Audit of the Information Systems General and Application Controls at Kaiser Foundation Health Plan, Inc., Northern and Southern California Regions

Rec. #2	***Finding***	Network Access Controls: Kaiser of CA does not have [redacted] controls to prevent [redacted]
	Recommendation	We recommend that Kaiser of CA complete its current project to implement [redacted]
	Status	This recommendation is resolved. Kaiser is taking corrective 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.

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. #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.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Consolidated Business Information System

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.

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.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative		
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.
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***	Federal Information Processing Standard (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.

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 – (Estech Systems, Inc.) ESI & LAN/WAN General Support Systems: In the most recent Authorizations, the ESI GSS's PTA (Privacy Threat Analysis)was not complete (i.e., it did not indicate whether a PIA [Privacy Impact Assessment] 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. #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.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative		
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.
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.

Title: Federal Information Security Modernization Act Audit FY 2019 **Report #: 4A-CI-00-19-029** **Date: October 29, 2019**		
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.
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.

Continued: Federal Information Security Modernization Act Audit FY 2019		
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.
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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2019

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.
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.

* represents repeat recommendations.

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.
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.

* represents repeat recommendations.

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. #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. #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.

Continued: Federal Information Security Modernization Act Audit FY 2019		
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.
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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2019		
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. #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.

* represents repeat recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2019		
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.
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.

Title: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Electronic Official Personnel Folder System **Report #: 4A-CI-00-20-007** **Date: June 30, 2020**		
Rec. #2	***Finding***	Contingency Plan: In April 2019, OPM was able to move the Electronic Official Personnel Folder (eOPF) backup systems to Boyers, Pennsylvania as originally planned. However, the eOPF Contingency Plan has not been updated to reflect the change in backup location.
	Recommendation	We recommend that OPM update the eOPF Contingency Plan in accordance with 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.

* represents repeat recommendations.

Continued: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Electronic Official Personnel Folder System

Rec. #3	***Finding***	Contingency Plan Testing: However, no contingency plan test was conducted in FY 2019. The potential consequences of not performing the contingency plan test in FY 2019 are compounded by the fact that the backup systems were recently moved and no testing has been performed to ensure that eOPF can be restored at the new location.
	Recommendation	We recommend that OPM conduct a test of the updated eOPF Contingency Plan in accordance with OPM policies. Note: This recommendation cannot be implemented until the Contingency Plan is updated as a part of the corrective action for Recommendation 2.
	Status	OPM is taking corrective 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 Information Systems General and Application Controls at the National Association of Letter Carriers Health Benefit Plan
Report #: 1B-32-00-20-004
Date: September 9, 2020

Rec. #8	***Finding***	Internal Network Segmentation: National Association of Letter Carriers Health Benefit Plan (NALC HBP) uses firewalls to control connections with systems outside of its network as well as between public-facing applications and the internal network. [redacted]
	Recommendation	We recommend that NALC HBP [redacted]
	Status	This recommendation is resolved. NALC is taking corrective 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. #9	***Finding***	Network Access Control: NALC HBP's "Network Security Management Policy" states that only authorized computers will be able to access the internal network. [redacted]
	Recommendation	We recommend that NALC HBP [redacted]
	Status	This recommendation is resolved. NALC is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Audit of the Information Systems General and Application Controls at the National Association of Letter Carriers Health Benefit Plan		
Rec. #10	***Finding***	Vulnerability Scanning: [redacted]
	Recommendation	We recommend that NALC HBP [redacted]
	Status	This recommendation is resolved. NALC is taking corrective 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. #12	***Finding***	Network Monitoring: [redacted]
	Recommendation	We recommend that NALC HPB [redacted]
	Status	This recommendation is resolved. NALC is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for monitoring network activity for abnormal events.
Rec. #16	***Finding***	Business Continuity Plan Testing: NALC HBP's business continuity plan includes an alternate facility at which personnel can continue business operations, such as claims processing, in the event the primary location becomes unavailable. [redacted].
	Recommendation	We recommend that NALC HBP [redacted]
	Status	This recommendation is resolved. NALC is taking corrective 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.

Continued: Audit of the Information Systems General and Application Controls at the National Association of Letter Carriers Health Benefit Plan		
Rec. #17	***Finding***	Disaster Recovery Plan Testing: NALC HBP's disaster recovery plan includes a detailed process to recover critical IT infrastructure and applications at an alternate location. [redacted]
	Recommendation	We recommend that NALC HBP [redacted]
	Status	This recommendation is resolved. NALC is taking corrective 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 Security Assessment and Authorization Methodology Report #: 4A-CI-00-20-009 Date: September 18, 2020		
Rec. #1	***Finding***	Authorization Memorandum: All of the systems we reviewed have a valid Authorization memorandum except for the Serena Business Manager (SBM). OPM did not reassess and authorize SBM prior to the most recent Autorization to Operate (ATO) expiration.
	Recommendation	We recommend that OPM perform a full assessment for SBM and update all Authorization documentation in accordance with NIST 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 ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #2	***Finding***	Incorrect System Categorization: Of the 15 FIPS 199 security categorization documents reviewed, two systems which were categorized as moderate-impact systems were identified as High Value Assets (HVA). The HVA worksheet identified a rating of high in either confidentiality or integrity for both systems. OPM contests that the HVA designation does not affect the system categorization. However, OPM's HVA template suggests otherwise.
	Recommendation	We recommend that OPM update its policies and procedures to include guidance on categorizing HVA systems.
	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.

Continued: Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology		
Rec. #3	***Finding***	Missing Approvals: We observed seven security categorization documents that were not signed by all necessary personnel.
	Recommendation	We recommend that OPM have the System Owner (SO), the Chief Information Security Officer (CISO), the Authorizing Official (AO), and (where appropriate) the Chief Privacy Officer review and approve the categorization of the systems in its inventory, in accordance with agency 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 ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #4	***Finding***	System Security Plan: We reviewed the SSP and master control set of the 15 systems in scope. Our fieldwork indicates that the SSPs are not being reviewed and updated timely because OPM does not have an SSP review process in place for the Information System Security Officers (ISSO).
	Recommendation	We recommend that OPM develop and implement a process to perform annual quality reviews for SSPs. The process should include the elements defined in NIST SP 800-18, Revision 1.
	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 systems have appropriate security controls in place and functioning properly.
Rec. #5	***Finding***	Master Control Set: Of the 15 systems reviewed, 7 systems had master control set fields that were incomplete or missing and contained planned controls that did not have corresponding POA&M references. The ISSOs are not updating all fields of the master control set appropriately with all defined controls.
	Recommendation	We recommend that OPM routinely ensure that all SSP master control sets are updated with POA&M references.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology		
Rec. #6	***Finding***	Security Assessment Plan and Report: OPM's ISSOs appear unable to provide consistent oversight of the security control assessment to ensure that all required controls are assessed for risk and weaknesses are identified. This issue is compounded by the inaccuracies in the system security categorization and SSP.
	Recommendation	We recommend that OPM improve the training program for new and current ISSOs on OPM's Authorization process. Training should include guidance on how to provide proper oversight related to security control scoping and risk identification and documentation.
	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 performing Security Assessment and Authorizations.
Rec. #7	***Finding***	Contingency Plan: We reviewed the CP and Business Impact Analysis (BIA) for the 15 systems in our audit scope. The SO is not completing a sufficiently detailed review of contingency planning documents at the agency defined frequency or in the event of a system change to ensure the accuracy of information and compliance with contingency planning controls.
	Recommendation	We recommend that OPM implement a contingency plan review process to ensure the accuracy of information and compliance with contingency planning controls.
	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. #8	***Finding***	Business Impact Analysis: Two of the system BIAs were performed by a contractor. The contractor performed the BIA based on its business process as it relates to its mission. The analysis performed by the contractor does not mention OPM nor the impact of the system on the agency.
	Recommendation	We recommend that OPM develop and implement a process that ensures SOs of contractor-operated systems work with internal process owners, leadership and business managers to create an OPM BIA.
	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 assessing and documenting system criticality.

Continued: Audit of the U.S. Office of Personnel Management's Security Assessment and Authorization Methodology		
Rec. #9	***Finding***	Contingency Plan Testing: OPM does not have a template for CP testing so it is up to the SO to define what to test and what information to report in the test's after action report. During the FY 2019 FISMA audit, we identified that CP testing was not performed annually for all OPM systems. Additionally, we observed three systems that did not have the sufficient scope appropriate for the security categorization of the system. All three systems only performed table-top CP tests.
	Recommendation	We recommend that OPM adhere to the guidance in its Contingency Planning Policy and conduct full-scale tests for high-impact systems, functional tests for moderate-impact systems, and table-top tests for low-impact systems 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.
Rec. #10	***Finding***	Plan of Action and Milestones: While OPM has adequate policies and procedures in place for its POA&M process, ISSOs are not effectively updating POA&Ms with adequate information. Of the 361 POA&Ms reviewed, 109 were still in an initial or draft status more than six months after the creation date. Initial and draft POA&Ms did not yet contain all of the information required (e.g., milestones, estimated completion dates, estimated costs and labor) for managing POA&Ms and remediating weaknesses cost effectively.
	Recommendation	We recommend that OPM document the required milestone information so that the identified POA&Ms can be moved to an open status.
	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. #11	***Finding***	Plan of Action and Milestones: Of the 361 POA&Ms reviewed, 109 were still in an initial or draft status more than six months after the creation date. Initial and draft POA&Ms did not yet contain all of the information required (e.g., milestones, estimated completion dates, estimated costs and labor) for managing POA&Ms and remediating weaknesses cost effectively.
	Recommendation	We recommend that OPM update its POA&M procedures to include timeliness metrics related to transitioning a POA&M from initial/draft status to open.
	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.

Title: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Agency Common Controls **Report #: 4A-CI-00-20-008** **Date: October 18, 2020**		
Rec. #1	***Finding***	Policy and Procedures Governing the CSCC: The Use of the Common Security Controls Collection document defines the CSCC and provides instructions for Information System Security Officers (ISSOs) to determine which controls in their system are part of the CSCC and to not include those controls in a system security controls assessment. A 2013 Memorandum to System Owners (SOs) and Designated Security Officers regarding the CSCC stated that certain controls would no longer be part of the CSCC and issued a revised version of the CSCC. Upon completing our review of provided documentation, we did not observe any mention of the CSCC assessment requirements or roles, and responsibilities as conveyed by OPM representatives during our fieldwork interviews
	Recommendation	We recommend that OPM document the governance requirements of the CSCC that at a minimum contain the following elements as stated by NIST: a) Assigns responsibilities for oversight of the CSCC; b) Mandates the same assessment and monitoring requirements as system-specific controls in OPM information systems; and c) Requires the communication of assessment results to SOs and ISSOs.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for the transition of a system's management.
Rec. #2	***Finding***	Plan of Action and Milestones: The 33 deficient controls identified in the risk assessment were not tracked through POA&Ms nor were they communicated to the ISSOs, SOs, or AOs of the systems that inherit the controls. OPM officials stated that no POA&Ms relating to the CSCC deficiencies were listed in the official document repository. OPM officials also stated that "artifacts on the communications to ISSOs or SOs could not be found."
	Recommendation	We recommend that OPM conduct an independent assessment of the controls that make up the CSCC.
	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: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Agency Common Controls		
Rec. #3	***Finding***	Plan of Action and Milestones: Since the assessment of the CSCC controls did not properly document the risk assessment of the deficient controls and POA&Ms of the deficient controls were not documented nor communicated, the AOs did not receive all of the information to properly assess the risks to their systems. Conducting a new independent assessment of the CSCC controls would provide OPM the opportunity to address the identified documentation issues and properly document the assessment.
	Recommendation	We recommend that OPM update the CSCC to accurately reflect the controls in place and provided to the agency's systems.
	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 POA&M weakness remediation.
Rec. #4	***Finding***	CSCC Controls Testing: The 2017 CSCC assessment results were not communicated to ISSOs, SOs, or AOs whose systems inherit these controls. The CSCC contains agency common controls that are inherited by all OPM systems and are therefore not required to be tested as part of individual system security control assessments.
	Recommendation	We recommend that OPM notify all Authorizing Officials of the status of the controls identified from the CSCC that are not fully implemented.
	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 conducting risk assessments.

Title: Federal Information Security Management Act Audit FY 2020 **Report #: 4A-CI-00-20-010** **Date: October 30, 2020**		
Rec. #4*	***Finding***	Hardware Inventory: OPM's Security Authorization Guide says that in order to register OPM systems, hardware assets included in its system boundary are documented and electronically maintained. However, OPM does not have a defined process to maintain its inventory of hardware assets.
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020		
Rec. #6*	***Finding***	Software Inventory: OPM has a policy that requires software components to be inventoried. However, a documented process to maintain software inventory is still not in place. Defining data elements to include in a software inventory would improve OPM's tracking of software in its environment. Further, instances of unsupported software were found during our testing. OPM purchased a tool this year that when implemented could address these concerns.
	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: OPM has a policy that requires software components to be inventoried. However, a documented process to maintain software inventory is still not in place. Defining data elements to include in a software inventory would improve OPM's tracking of software in its environment. Further, instances of unsupported software were found during our testing. OPM purchased a tool this year that when implemented could address these concerns.
	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. #9*	***Finding***	Risk Policy and Strategy: OPM's Risk Management and Internal Controls Council manages the Enterprise Risk Management program. The Council meets regularly to discuss various risk topics and update the agencies risk profile. However, OPM has not incorporated supply chain risk management (SCRM) in its risk strategies. OPM has identified funding as an issue in developing an action plan to address supply chain requirements.
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020		
Rec. #10*	***Finding***	Information Security Architecture: OPM has guidance for implementing an information security architecture. The information security architecture is meant to be a plan for the implementation of security mechanisms. OPM's Enterprise Architecture has not been updated since 2008, and it does not contain a Security Reference Model, which represents the agency's information security architecture. OPM also has an Enterprise Information Security Architecture, however the document is in draft form.
	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.
Rec. #12*	***Finding***	Plan of Action and Milestones: OPM's OCIO has now prioritized POA&Ms, and stated that a new reporting feature in the POA&M repository alerts system owners of past due POA&Ms. As of July 31, 2020, we still noted the following issues: • 60 percent of open POA&Ms are past due; • 55 percent have not been updated in over a year; and • 11 percent have not been updated in three years.
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020		
Rec. #13*	***Finding***	Plan of Action and Milestones: OPM's OCIO has now prioritized POA&Ms, and stated that a new reporting feature in the POA&M repository alerts system owners of past due POA&Ms. As of July 31, 2020, we still noted the following issues: • 60 percent of open POA&Ms are past due; • 55 percent have not been updated in over a year; and • 11 percent have not been updated in three years.
	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	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. #14*	***Finding***	System Level Risk Assessments: In 2020, OPM began a project to document the system-level risk assessments in a consistent manner with enterprise-wide risk assessments. All new systems will participate in this new process, and existing systems will follow when their annual reviews occur. However, we have yet to receive any evidence from OPM to indicate that the OCIO's new process to perform risk assessments has been implemented.
	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***	Configuration Management Roles, Responsibilities, and Resources: OPM has indicated that it does not currently have adequate processes and technology to manage its CM program effectively. Additionally, OPM has not allocated the appropriate resources to perform a gap analysis that would assist in identifying areas of concern.
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020

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 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 analyzing and updating the agency's configuration management plan.
Rec. #19*	***Finding***	Baseline Configurations: 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 OPM develop and implement a baseline configuration for all information systems in use by OPM.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #21*	***Finding***	Security Configuration Settings: OPM has not consistently implemented the process for documenting and approving exceptions, which means OPM has not customized the configuration settings for its systems and environment. As a result, testing against the Guides is not effective since OPM has not documented 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	OPM is taking corrective 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. #23*	***Finding***	Security Configuration Settings: OPM has not consistently implemented the process for documenting and approving exceptions, which means OPM has not customized the configuration settings for its systems and environment. As a result, testing against the Guides is not effective since OPM has not documented the allowed deviations.
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020		
Rec. #27*	***Finding***	Flaw Remediation and Patch Management: OPM does not have a formal process to ensure all new devices in the environment are included in the scanning process. We also determined that not every device on OPM's network is scanned routinely
	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. #29*	***Finding***	ICAM Strategy: Last year, we determined that OPM had not developed or implemented an ICAM strategy containing milestones for how the agency plans to align with Federal ICAM initiatives. The ICAM strategy still has not been fully implemented, but OPM has contracted to assess the resource needs of the program. OPM expects to implement its ICAM strategy by June 2021.
	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. #33*	***Finding***	Data Protection and Privacy Policies and Procedures: The Chief Privacy Officer position was established in 2016. However, roles and responsibilities for the effective implementation of the agency's privacy program have not been defined. OPM's privacy program is relatively new and has not had sufficient resources devoted to it.
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020		
Rec. #34*	***Finding***	Data Protection and Privacy Policies and Procedures: The OPM Information Security and Privacy Policy Handbook continues to be the agency'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	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.
Rec. #35*	***Finding***	Data Breach Response Plan: As a part of the plan, a Breach Response Team has been established that includes the appropriate agency officials. OPM's breach response plan requires periodic testing and updating. However, this year OPM has not updated or tested its 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: OPM policy requires users to "Complete role-based security or privacy training if assigned a significant security or privacy role" and system owners to "Provide role-based security and privacy training to OPM information system users responsible for the operation of security functions/mechanisms for systems under his or her portfolio." However, OPM has not developed role-based privacy training for individuals
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020		
Rec. #41*	***Finding***	Contingency Planning Roles and Responsibilities: In FY 2019, OPM indicated that staffing constraints led to lapses in contingency plan maintenance and testing. This year we continue to see these constraints affect compliance with OPM policy as only a third of contingency plans were updated as required and less than a quarter were tested as required.
	Recommendation	We recommend that OPM perform a gap-analysis to determine the contingency planning requirements (people, processes, and technology) necessary to implement the agency's contingency planning policy effectively.
	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. #42*	***Finding***	Business Impact Analysis: OPM has not incorporated the results of this BIA into the system-level contingency plans. It is the responsibility of the system owners and Authorizing Officials to ensure that BIA results are communicated and reflected in system-level 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.
Rec. #43*	***Finding***	Contingency Plan Maintenance: While OPM has made progress, it is still not compliant with this policy. Only 16 of the 47 major systems have contingency plans that were reviewed and updated in FY 2020.
	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.

* represents repeat recommendations.

Continued: Federal Information Security Management Act Audit FY 2020

Rec. #44*	***Finding***	Contingency Plan Testing: During our testing only 11 of the 47 systems observed were subject to a contingency plan test in compliance with OPM policy.
	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.
Rec. #45	***Finding***	Information System Backup and Storage: We have not received evidence to indicate that OPM performs controls testing to ensure that the alternate storage and processing sites provide information security safeguards equivalent to that of the primary site. We reviewed 17 system security plans and observed that OPM did not consistently document the review of the alternate storage/processing site safeguards.
	Recommendation	We recommend that OPM perform and document controls testing to ensure security safeguards for alternate processing and storage sites are equivalent to the primary sites.
	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 recovering from an unplanned system outage.

Title: Audit of the Information Systems General and Application Controls at Health Alliance Plan of Michigan
Report #: 1C-52-00-20-011
Date: November 30, 2020

Rec. #1	***Finding***	Entity Segmentation: Health Alliance Plan ([redacted]
	Recommendation	[redacted]
	Status	This recommendation is resolved. HAP originally did not agree with the recommendation. However, HAP is now taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Audit of the Information Systems General and Application Controls at Health Alliance Plan of Michigan		
Rec. #7	***Finding***	Internal Network Segmentation: [redacted]
	Recommendation	[redacted]
	Status	This recommendation is resolved. HAP originally did not agree with the recommendation. However, HAP is now taking corrective 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. #10	***Finding***	Vulnerabilities Identified by OIG Scans: We conducted credentialed vulnerability and configuration compliance scans on a sample of servers and workstations in HAP's network environment. [redacted]
	Recommendation	[redacted]
	Status	HAP is taking corrective 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: Audit of the Information Systems General and Application Controls at Scott and White Health Plan **Report #: 1C-A8-00-20-019** **Date: December 14, 2020**		
Rec. #1	***Finding***	Vendor Risk Assessments: Baylor Scott and White Health (BSWH) Plan contracts with several vendors that perform business processes related to health claims processing. However, BSWH has not performed risk assessments of the IT security controls implemented by these vendors to protect the sensitive data they handle.
	Recommendation	We recommend that BSWH implement a formal process to assess vendor risk prior to service acquisition and then periodically over the course of the relationship. This process should also be applied to all existing vendors.
	Status	This recommendation is resolved. BSWH is taking corrective 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.

Continued: Audit of the Information Systems General and Application Controls at Scott and White Health Plan		
Rec. #2	***Finding***	Internal Network Segmentation: [redacted]
	Recommendation	We recommend that BSWH [redacted]
	Status	This recommendation is resolved. BSWH is taking corrective 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***	Network Access Control: [redacted]
	Recommendation	We recommend that BSWH [redacted]
	Status	This recommendation is resolved. BSWH is taking corrective 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***	Vulnerabilities Identified by OIG Scans: The specific vulnerabilities that we identified were provided to BSWH in the form of an audit inquiry, but will not be detailed in this report. The Plan has opened tickets for the vulnerabilities and begun taking appropriate actions.
	Recommendation	We recommend that BSWH remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.
	Status	This recommendation is resolved. BSWH is taking corrective 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.

Continued: Audit of the Information Systems General and Application Controls at Scott		
Rec. #10	***Finding***	Security Configuration Standards: The guides were developed internally and are maintained by BSWH personnel. [redacted]
	Recommendation	We recommend that BSWH document [redacted]
	Status	This recommendation is resolved. BSWH is taking corrective 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. #11	***Finding***	Security Configuration Standards: The guides were developed internally and are maintained by BSWH personnel. [redacted]
	Recommendation	We recommend that BSWH implement a process to [redacted]
	Status	This recommendation is resolved. BSWH is taking corrective 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. #12	***Finding***	Security Configuration Auditing: [redacted]
	Recommendation	We recommend that BSWH [redacted]
	Status	This recommendation is resolved. BSWH is taking corrective 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.

Title: Audit of the Information Systems General and Application Controls at Capital BlueCross **Report #: 1A-10-36-20-032** **Date: February 21, 2021**		
Rec. #1	***Finding***	Firewall Configuration Reviews: Firewalls are hardened to these best practices and any deviations are documented and tracked through the change management process. However, [redacted]
	Recommendation	We recommend that Capital BlueCross (CBC) perform [redacted].
	Status	This recommendation is resolved. CBC is taking corrective 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***	Vulnerabilities Identified by OIG Scans: CBC responded to our audit inquiry that it was aware of the majority of the vulnerabilities and those vulnerabilities were also identified in historical scan results that were provided. However, [redacted].
	Recommendation	We recommend [redacted]
	Status	This recommendation is resolved. CBC is taking corrective 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. #6	***Finding***	Security Configuration Auditing: Prior to systems being deployed, security configurations are applied in accordance with the approved configuration standards and reviewed for compliance using an automated tool. However, [redacted]
	Recommendation	We recommend [redacted]
	Status	This recommendation is resolved. CBC is taking corrective 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.

Title: Audit of the Information Systems General and Application Controls at Geisinger Health Plan
Report #: 1C-GG-00-20-026
Date: March 9, 2021

Rec. #1	***Finding***	Internal Network Segmentation: Geisinger Heath Plan (GHP) uses firewalls to control connections with systems outside of its network. GHP also utilizes virtual local area networks and firewalls to segment high risk or nonstandard devices from the rest of the network. However, GHP does not use firewalls to segment users from systems with sensitive information within the internal network.
	Recommendation	We recommend that GHP segregate its internal network in order to separate sensitive resources from user-controlled systems.
	Status	This recommendation is resolved. GHP is taking corrective 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. #2	***Finding***	Security Configuration Auditing: However, GHP does not routinely audit its system's security settings against its "Secure Configuration Guidelines" to ensure the actual settings on its systems are compliant with the approved settings.
	Recommendation	We recommend that GHP implement a process to routinely audit all server configuration settings to ensure compliance with the approved security configuration standards.
	Status	This recommendation is resolved. GHP is taking corrective 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.

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).[3]

Title: Audit of Claims Processing and Payment Operations at CareFirst BCBS **Report #: 1A-10-85-17-049** **Original Issue Date: October 23, 2019** **Corrected Report Issue Date: April 15, 2020**		
Rec. #1	***Finding***	Place of Service Overcharges Review: Our review identified $1,227,289 in program overcharges due to billing an incorrect place of service. These program overcharges also caused increased cost shares to some members and decreased cost shares to other members.
	Recommendation	We recommend that the contracting officer require the CareFirst Blue Cross Blue Shield (Plan) to return $1,227,289 in overcharges to the FEHBP.
	Status	This recommendation was resolved on March 10, 2020, meaning a plan for corrective action has been agreed to but not yet implemented. As of September 30, 2021, a balance of $546,817 was still owed to the FEHBP.
	Estimated Program Savings	$1,227,289
	Other Nonmonetary Benefit	N/A

[3] As defined in OMB Circular No. A-50, resolved means that the audit organization and agency management agree on action to be taken on reported findings and recommendations; however, corrective action has not yet been implemented. Outstanding and unimplemented (open) recommendations listed in this compendium that have not yet been resolved are not in compliance with the OMB Circular No. A-50 requirement that recommendations be resolved within six months after the issuance of a final report.

Title: Audit of Duplicate Claim Payments at all Blue Cross and Blue Shield Plans for the period July 1, 2016 through July 31, 2019
Report #: 1A-99-00-19-002
Date: February 12, 2021

Rec. # 2	***Finding***	Duplicate Claim Payments: Our review determined that the local Blue Cross Blue Shield (BCBS) plans incorrectly paid 986 claims totaling $2,095,900 in health benefit net overcharges to the FEHBP. Specifically, 973 claims were overpaid by $2,126,618 and 13 claims were underpaid by $30,718.
	Recommendation	We recommend that the Association work with its local BCBS plans to review system issues within their systems and/or within the FEPDirect system that have allowed duplicates such as these to occur. Specifically, they should focus on why these claims were not deferred prior to payment.
	Status	This recommendation was resolved on August 2, 2021, meaning a plan for corrective action has been agreed to but not yet implemented. Milestone M-4 of the Association's corrective action plan, related to recommendation #2, still needs to be completed before this recommendation can be closed.
	Estimated Program Savings	Unknown
	Other Nonmonetary Benefit	While an actual monetary amount is hard to estimate, if the root cause of these improper payments is identified and appropriate actions are implemented, it will prevent the improper payment of these types of claims going forward.
Rec. #3	***Finding***	Duplicate Claim Payments: Our review determined that the local BCBS plans incorrectly paid 986 claims totaling $2,095,900 in health benefit net overcharges to the FEHBP. Specifically, 973 claims were overpaid by $2,126,618 and 13 claims were underpaid by $30,718.
	Recommendation	We recommend that the Association work with it local BCBS plans to review and correct system issues (either at the local level or in FEPDirect) that have permitted duplicate claim payments to go undetected.
	Status	This recommendation was resolved on August 2, 2021, meaning a plan for corrective action has been agreed to but not yet implemented. Milestone M-4 of the Association's corrective action plan, related to recommendation #3, still needs to be completed before this recommendation can be closed.
	Estimated Program Savings	Unknown
	Other Nonmonetary Benefit	While an actual monetary amount is hard to estimate, if the root cause of these improper payments is identified and appropriate actions are implemented, it will prevent the improper payment of these types of claims going forward.

Title: Audit of Enrollment at All Blue Cross and Blue Shield Plans for Contract Years 2018-2019 **Report #: 1A-99-00-20-018** **Date: March 12, 2021**		
Rec. #3	***Finding***	Retroactive Eligibility Updates: Our review identified 38 members that were ineligible for coverage at the time claims were incurred, based on retroactive eligibility updates. These members incurred 388 claims (medical and pharmacy) totaling $388,704 in erroneous payments. Of the 38 members 13 appeared to be either former spouses or ineligible dependents. For these 13 members, in addition to the erroneous payments incurred by them, our review showed that, on average, coverage continued for them for 10 years after FEHBP guidance deemed them ineligible.
	Recommendation	We recommend that the Association direct its local BCBS plan SIUs to instruct processors on how to identify, review, and report the type of potential enrollment fraud identified in this finding as possible Fraud, Waste, and Abuse cases.
	Status	This recommendation was resolved on August 12, 2021, meaning a plan for corrective action has been agreed to but not yet implemented. Milestones 5 & 6 of the Association's corrective action plan still needs to be completed and evidence of their completion needs to be provided to OPM before this recommendation can be closed.
	Estimated Program Savings	Unknown
	Other Nonmonetary Benefit	While an actual monetary amount is hard to estimate, if appropriate actions are put in place to properly identity and remove these ineligible members, it will prevent the improper payment of these types of claims going forward.

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 CareFirst BlueChoice's FEHBP Pharmacy Operations as Administered by CVS Caremark **Report #: 1H-07-00-19-017** **Date: July 20, 2020**		
Rec. #2	***Finding***	The Pharmacy Benefit Manager (PBM) did not provide pass-through transparent pricing based on the full value of the discounts it negotiated with two retail pharmacies for contract years (CY) 2014 through 2016, resulting in an overcharge of $834,425 to the FEHBP.
	Recommendation	We recommend that the PBM return $834,425 to the Carrier (to be credited to the FEHBP) for failing to provide pass-through pricing to the FEHBP at the full value of the PBM's negotiated discounts with Walgreens and Rite Aid retail pharmacy claims for CYs 2014 through 2016.
	Status	The Carrier and the PBM continue to disagree with this recommendation. The agency is reviewing the Carrier's position and will provide a response in the future.
	Estimated Program Savings	$834,425
	Other Nonmonetary Benefit	Establishes controls to ensure the carrier is compliant with FEHBP PBM transparency standards.
Rec. #3	***Finding***	The PBM did not provide pass-through transparent pricing based on the full value of the discounts it negotiated with two retail pharmacies for CYs 2014 through 2016, resulting in an overcharge of $834,425 to the FEHBP.
	Recommendation	We recommend that the PBM continue researching this issue and identify all other pharmacies whose full value of the negotiated discounts were not passed through to the FEHBP.
	Status	The Carrier and the PBM continue to disagree with this recommendation. The agency is reviewing the Carrier's position and will provide a response in the future.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls to ensure the carrier is compliant with FEHBP PBM transparency standards.

Continued: Audit of CareFirst BlueChoice's FEHBP Pharmacy Operations as Administered by CVS Caremark		
Rec. #4	***Finding***	The PBM did not provide pass-through transparent pricing based on the full value of the discounts it negotiated with two retail pharmacies for CYs 2014 through 2016, resulting in an overcharge of $834,425 to the FEHBP.
	Recommendation	We recommend that the Carrier require the PBM to pay FEHBP pharmacy claims based on the full value of the PBM's negotiated discounts with retail pharmacies at the time of adjudication. The guarantee found in the Agreement (between the Carrier and the PBM) should only be applied as a true-up when that guaranteed discount exceeds the pass-through transparent pricing for the period being analyzed.
	Status	The Carrier and the PBM continue to disagree with this recommendation. The agency is reviewing the Carrier's position and will provide a response in the future.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls to ensure the carrier is compliant with FEHBP PBM transparency standards.
Rec. #5	***Finding***	The PBM did not provide pass-through transparent pricing based on the full value of the discounts it negotiated with two retail pharmacies for CYs 2014 through 2016, resulting in an overcharge of $834,425 to the FEHBP.
	Recommendation	We recommend that the Carrier require the PBM to provide annual comparisons and/or true ups showing that the FEHBP received the larger discount of either the guarantee found in the Agreement (between the Carrier and the PBM) or the pass-through transparent pricing equal to the full value of the PBM's negotiated discounts with retail pharmacies.
	Status	The Carrier and the PBM continue to disagree with this recommendation. The agency is reviewing the Carrier's position and will provide a response in the future.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls to ensure the carrier is compliant with FEHBP PBM transparency standards.
Rec. #6	***Finding***	The PBM did not provide pass-through transparent pricing based on the full value of the discounts it negotiated with two retail pharmacies for CYs 2014 through 2016, resulting in an overcharge of $834,425 to the FEHBP.
	Recommendation	We recommend that the PBM adopt controls to ensure that the FEHBP always receives pass-through transparent pricing. Controls should include an annual check to ensure that the FEHBP received, at a minimum, the full value of the PBM's negotiated discounts with retail pharmacies.
	Status	The Carrier and the PBM continue to disagree with this recommendation. The agency is reviewing the Carrier's position and will provide a response in the future.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls to ensure the carrier is compliant with FEHBP PBM transparency standards.

Title: Audit of the U.S. Office of Personnel Management’s Administration of Federal Employee Insurance Programs
Report #: 4A-HI-00-19-007
Date: October 30, 2020

Rec. #1	***Finding***	We found that OPM had three contracting officers (CO) administering healthcare and insurance contracts without evidence of completing the required training.
	Recommendation	We recommend that the three COs obtain the proper training to meet the 80 continuous learning points (CLP) requirement every two years and submit the training certificates in FAITAS.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Establishes controls to ensure OPM is compliant with Federal Acquisition Certification in Contracting (FAC-C) Level III CLPs.
Rec. #2	***Finding***	We found that OPM had three COs administering healthcare and insurance contracts without evidence of completing the required training.
	Recommendation	We recommend that OPM develop policies and procedures to strengthen its monitoring and oversight of training related to CO warrants to ensure that the warrants are rescinded if certification of 80 CLPs every two years is not documented in FAITAS.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Establishes controls to ensure OPM is compliant with Federal Acquisition Certification in Contracting (FAC-C) Level III CLPs.
Rec. #3	***Finding***	We found that OPM had health insurance specialists and program analysis officers acting in the capacity of a contracting officer representative (COR) without the proper letter of designation, certification, or training.
	Recommendation	We recommend that OPM require its health insurance specialists and program analysis officers within its Federal Employees Insurance Office (FEIO), who are acting in the capacity of a COR, to obtain the proper Federal Acquisition Certification for Contracting Officer’s Representatives (FAC-COR) designation.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Establishes controls to ensure OPM is compliant with FAC-COR requirements.

Continued: Audit of the U.S. Office of Personnel Management's Administration of Federal Employee Insurance Programs		
Rec. #4	***Finding***	We found that OPM had health insurance specialists and program analysis officers acting in the capacity of a Contracting Officer's Representative (COR) without the proper letter of designation, certification, or training.
	Recommendation	We recommend that OPM require each COR to obtain a letter of designation from the CO that describes their duties and responsibilities, a copy of the contract administration functions delegated to a contract administration office which may not be delegated to the COR, and documentation of COR actions taken in accordance with the delegation of authority.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Establishes controls to ensure OPM is compliant with FAC-COR requirements.
Rec. #5	***Finding***	We found that Audit Resolution and Compliance (ARC) lacks the resources and support needed to timely resolve OIG audit recommendations in accordance with the requirements of OMB Circular No. A-50. Our review found that ARC failed to resolve audit recommendations in 114 out of 246 audits, or approximately 46 percent, within the six-month period after the report was issued by the OIG. Of the 114 audits with recommendations that were not resolved within six months, 11 audits with 29 recommendations remained open at the time of our review, including 12 monetary recommendations with over $103 million in questioned costs.
	Recommendation	We recommend that OPM provide ARC with a new audit resolution system that tracks, records, and reports resolution transactions.
	Status	OPM partially concurs with the recommendation and asserts that OPM should acquire an agency-wide audit resolution system that records and tracks recoveries and resolutions, and reports and performs analyses on resolutions to be shared by OPM's Healthcare and Insurance Office (HIO), the Office of the Chief Financial Officer (OCFO), the OIG and Internal Oversight and Compliance (IOC). The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Establishes controls to ensure OPM is compliant with the requirements of OMB Circular No. A-50 for resolving OIG audit recommendations.

Continued: Audit of the U.S. Office of Personnel Management's Administration of Federal Employee Insurance Programs		
Rec. #6	***Finding***	We found that ARC lacks the resources and support needed to timely resolve audit recommendations in accordance with the requirements of OMB Circular No. A-50. Our review found that ARC failed to resolve audit recommendations in 114 out of 246 audits, or approximately 46 percent, within the six-month period after the report was issued by the OIG. Of the 114 audits with recommendations that were not resolved within six months, 11 audits with 29 recommendations remained open at the time of our review, including 12 monetary recommendations with over $103 million in questioned costs.
	Recommendation	We recommend that OPM provide ARC with the proper staffing and training needed to resolve audit recommendations timely based on an assessment of the workload, critical skills, and core competencies required to be knowledgeable in each of OPM's employee benefit programs.
	Status	OPM agrees that ARC needs additional resources to properly resolve audit recommendations in accordance with OMB Circular No. A-50. However, they disagree that ARC lacks the competencies required to be knowledgeable in the benefit programs that HIO administers. The OIG has not yet received evidence that corrective actions have been taken.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Establishes controls to ensure OPM is compliant with the requirements of OMB Circular No. A-50 for resolving OIG audit recommendations.
Rec. #9	***Finding***	During our review of OPM's current policies and procedures for collecting and reviewing FEHBP carrier Annual Accounting Statements (AAS), we found that OPM had insufficient oversight of the FEHBP carriers' working capital. Specifically, OPM is not verifying that the working capital schedule is being submitted with the carriers' AAS or tracking each carrier's working capital balance.
	Recommendation	We recommend that OPM work with the OCFO to establish internal procedures for properly reviewing and verifying the accuracy and completeness of the working capital schedules reported in the AAS by Fee-for-Service (FFS) and Experience-Rated (ER) Health Maintenance Organization (HMO) carriers.
	Status	This recommendation was resolved on September 21, 2021, meaning a plan for corrective action has been agreed to but not yet implemented.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Establishes controls over the working capital schedules reported in the AAS by FFS and ER HMO carriers participating in the FEHBP.
Rec. #11	***Finding***	OPM lacks standards in its community-rated HMO contracts to ensure transparency of costs charged by PBMs.
	Recommendation	We recommend that OPM establish PBM transparency standards for all new, renewed, or amended contracts that are specific to community-rated HMOs.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls over the pharmacy operations for community-rated HMOs participating in the FEHBP.

Continued: Audit of the U.S. Office of Personnel Management's Administration of Federal Employee Insurance Programs		
Rec. #12	***Finding***	We found that OPM's Medical Loss Ratio (MLR) regulations and criteria are insufficient to address issues stemming from health insurers that are owned by provider groups and health care systems (provider-sponsored plans). Specifically, the lack of criteria addressing provider-sponsored plans affords them the opportunity to shift profit and/or expenses down to the provider level through increased claims costs, while still meeting the 85 percent MLR requirement.
	Recommendation	We recommend that OPM implement the following rate instruction changes: • Include transparency standards requiring the carriers to provide support for all claims, encounters, and capitated rates, including those from their provider-owned networks or related entities used in the MLR, rate proposal, and rate reconciliation calculations; and • Improve MLR criteria to provide complete, clear, and concise instructions of the FEHBP MLR process, including specific instructions concerning provider-sponsored health plans and capitated arrangements in its cost reporting.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Tightens controls related to MLR for community-rated provider-sponsored plans participating in the FEHBP so that the 85 percent MLR requirement is not circumvented.
Rec. #13	***Finding***	We found that FEIO is not conducting carrier site visits every three years as reported by the OCFO as an internal control to mitigate risk over the FEHBP payment process.
	Recommendation	We recommend that OPM develop formal policies to ensure that site visits are conducted every three years for FEHBP carriers in accordance with its control to meet OMB Circular A-123 requirements. If the time and costs to perform the site visits outweigh the benefits, OPM should modify its controls and report new procedures to mitigate risks in the FEHBP payment process.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls to meet the requirements of OMB Circular A-123 for oversight of the FEHBP payment process.
Rec. #15	***Finding***	During our review of OPM's current policies and procedures for ensuring carrier compliance with FWA reporting requirements, we found that OPM's health insurance specialists did not perform sufficient reviews of the 2017 FEHBP carriers' Fraud and Abuse Reports that were submitted in 2018. In addition, OPM did not have controls in place to hold carriers accountable for the timely submission of reports.
	Recommendation	We recommend that OPM implement a tracking mechanism to log the receipt of annual Fraud and Abuse Reports and hold FEHBP carriers accountable for the timely submission of their reports.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Strengthens controls over of the FEHBP FWA reporting requirements.

Continued: Audit of the U.S. Office of Personnel Management's Administration of Federal Employee Insurance Programs		
Rec. #16	***Finding***	OPM has no controls in place to verify family member relationships for FEDVIP. Instead, Federal employees and annuitants "self-certify" the eligibility of members they want added to their dental and vision plans.
	Recommendation	We recommend that OPM eliminate the self-certification process for FEDVIP and implement an enrollment verification process that requires documentation to prove family member relationships at the time of enrollment. In the meantime, BENEFEDS, as the sole enrollment portal for FEDVIP, should have the authority to request eligibility documentation that includes marriage and birth certificates.
	Status	OPM disagrees with the recommendation and therefore has taken no action.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls over of the FEDVIP eligibility requirements and reduces the risk of FWA in the program.
Rec. #22	***Finding***	OPM does not have a set of standardized performance metrics or penalties to hold FEDVIP carriers accountable for services provided to its members.
	Recommendation	We recommend that OPM develop standard performance metrics with penalties to be included in all new or renewed contracts with FEDVIP carriers.
	Status	OPM partially concurs, however no corrective action has been taken to implement the recommendation.
	Estimated Program Savings	Indirect savings – unknown, potentially significant.
	Other Nonmonetary Benefit	Establishes controls over of the accountability, consistency, quality, and level of service provided by carriers to FEDVIP members.

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 the 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 the 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 Qualifications Review Board (QRB) data.
	Recommendation	The OIG recommends 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 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 recommends 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 the 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. #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 recommends 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 the 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.
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 recommends 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 the recommendation. The OIG has not yet received evidence that the 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 aligned 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 recommends 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	The agency agreed with the 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.
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 recommends 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 recommends 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	The agency agreed with the 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 recommends 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	The agency agreed with the 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.

VI. Management Advisories and Other Reports

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

Title: Review of the U.S. Office of Personnel Management's Compliance with the Freedom of Information Act **Report #: 4K-RS-00-14-076** **Date: March 23, 2015**		
Rec. #1	***Finding***	Compliance with Electronic Freedom of Information Act Amendments of 1996 (EFOIA) - OPM's FOIA policy does not discuss the requirement to post information online that has been requested multiple times. In addition, OPM's request tracking system does not identify the type of information requested. Consequently, OPM's FOIA Office cannot identify multiple requests that should be posted.
	Recommendation	The OIG recommends that OPM's FOIA Office document a formal policy for handling multiple requests of the same information.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A.
	Other Nonmonetary Benefit	Improved internal controls for managing FOIA requests
Rec. #3	***Finding***	Compliance with Electronic Freedom of Information Act Amendments of 1996 E-FOIA requires agencies to provide online reading rooms for citizens to access records and, in the instance of three or more requests for certain FOIA information that this information be posted in these rooms. OPM's website has a reading room that OPM's FOIA Office can use to post responses to multiple requests; however, we found that the reading room is not used.
	Recommendation	The OIG recommends that OPM's FOIA Office start tracking types of FOIA requests to help determine whether they are multiple requests that must be posted to the reading room.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved internal controls for managing FOIA requests

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

Title: Delegation of Authority to Operate and Maintain the Theodore Roosevelt Federal Building and the Federal Executive Institute
Report #: 4A-DO-00-20-041
Date: August 5, 2020

Rec. #1	***Finding***	The decision to revoke OPM's authority to operate and maintain the Theodore Roosevelt Federal Building (TRB) and the Federal Executive Institute (FEI) was not well planned. A comprehensive analysis of the costs associated with the revocation of the delegation, including the costs associated with and any potential savings from a decrease in space utilization was not completed. Despite this lack of analysis and understanding of the true cost, and despite the preliminary analysis completed by OPM showing a significant increase in costs for the TRB, OPM and GSA initiated the process to transfer the operation and maintenance of both the TRB and the FEI to GSA, including solicitations for consolidated operation and management services.
	Recommendation	We recommend that OPM work with GSA to formally request and complete the documentation necessary to effectuate the return of the delegation to operate and maintain the TRB to OPM.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Savings	$14.4 million with $4.2 million recurring.
	Other Nonmonetary Benefit	N/A
Rec. #2	***Finding***	See number 1.
	Recommendation	We recommend that OPM delay any feasibility study related to its space needs until after completion of the NAPA study and any resulting decision by Congress
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	Unknown,
	Other Nonmonetary Benefit	N/A
Rec. #4	***Finding***	See number 1.
	Recommendation	We recommend that once the delegation to operate and maintain the FEI is returned, OPM explore its options regarding security services for the campus, including the potential return of the delegation from the Department of Homeland Security's Federal Protective Services, to determine if cost savings can be regained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	$300,000,
	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	14	0	$0
4A-CF-00-17-012	FY 2016 IPERA	5/11/2017	10	1	0	$0
4A-CF-00-17-028	FY 2017 Financial Statements	11/13/2017	18	15	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

Internal Audits Continued

Report Number	Name	Date	Total # of Recs.	# of Open Procedural Recs.	Monetary Findings	
4A-CF-00-19-012	FY 2018 IPERA	6/3/2019	4	3	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
4A-RS-00-18-035	IP Rate Methodologies	4/2/2020	12	12	0	$0
4A-CF-00-20-014	FY 2019 IPERA	5/14/2020	3	3	0	$0
4A-RS-00-19-038	U.S. Office of Personnel Management's Retirement Services Disability Process in Washington, D.C.	10/30/2020	8	8	0	$0
4A-CF-00-20-024	FY 2020 Financial Statements	11/13/2020	21	21	0	$0
25	Total Reports		232	165	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	1	0	$0
4A-CI-00-09-031	FISMA FY 2009	11/05/2009	30	1	0	$0
4A-CI-00-10-019	FISMA FY 2010	11/10/2010	41	1	0	$0
4A-CI-00-11-009	FISMA FY 2011	11/09/2011	29	1	0	$0
4A-CI-00-12-016	FISMA FY 2012	11/05/2012	18	1	0	$0
4A-CI-00-13-021	FISMA FY 2013	11/21/2013	16	1	0	$0
4A-CI-00-14-016	FISMA FY 2014	11/12/2014	29	3	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	3	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	5	0	$0

Information System Audits Continued

Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
1C-JP-00-16-032	ISG&AC @ UnitedHealthcare	1/24/2017	2	1	0	$0
4A-CI-00-17-014	OPM's Security Assessment & Authorization	06/20/2017	4	3	0	$0
1C-GA-00-17-010	ISG&AC @ MVP Health Care	6/30/2017	15	1	0	$0
4A-CI-00-17-030	OPM's SharePoint Implementation	09/29/2017	8	7	0	$0
4A-CI-00-17-020	FISMA FY 2017	10/27/17	39	14	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
1C-PG-00-17-045	ISG&AC @ Optima Health Plan	5/10/2018	20	1	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	21	0	$0
1C-UX-00-18-019	ISG&AC @ Medical Mutual of Ohio	1/24/2019	12	1	0	$0
1C-8W-00-18-036	ISG&AC @ UPMC	3/1/2019	5	1	0	$0
1C-LE-00-18-034	ISG&AC @ Priority Health	3/5/2019	10	1	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	3	0	$0
1C-59-00-19-005	ISG&AC @ Kaiser Northern and Southern California	7/23/2019	2	2	0	$0
4A-CF-00-19-026	OPM's CBIS	10/3/2019	7	3	0	$0
4A-CI-00-19-008	OPM's Compliance with Data Center Optimization	10/23/2019	23	13	0	$0
4A-CI-00-19-029	FISMA FY 2019	10/29/2019	47	23	0	$0
4A-CI-00-20-007	OPM's eOPF	06/30/2020	3	2	0	$0
1B-32-00-20-004	ISG&AC @ NALC	09/09/2020	19	6	0	$0
4A-CI-00-20-009	OPM's Security Assessment & Authorization	09/18/2020	11	11	0	$0

Information System Audits Continued						
Report Number	**Name**	**Date**	**Total # of Findings**	**# of Open Procedural Findings**	**Monetary Findings**	
					# Open	**Amount**
4A-CI-00-20-008	OPM's Agency Common Controls	10/30/2020	4	4	0	$0
4A-CI-00-20-010	FISMA FY 2020	10/30/2020	45	24	0	$0
1C-52-00-20-011	ISG&AC @ Health Alliance Plan	11/30/2020	14	3	0	$0
1C-A8-00-20-019	ISGC @ Scott and White Health Plan	12/14/2020	12	7	0	$0
1A-10-36-20-032	ISG&AC @ Capital BlueCross	2/21/2021	7	3	0	$0
1C-GG-00-20-026	ISGC @ Geisinger Health Plan	3/9/2021	2	2	0	$0
40	**Total Reports**		637	188	0	$0

Claim Audits and Analytics						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**Monetary Findings**	
					# Open	**Amount**
1A-10-85-17-049	Audit of Claims Processing and Payment Operations at CareFirst BCBS	10/23/2019 4/15/2020	10		1	$1,227,289
1A-99-00-19-002	Audit of Duplicate Claim Payments at All Blue Cross Blue Shield Plans for the period July 1, 2016, through July 31, 2019	2/12/21	8	2		
1A-99-00-20-018	Audit of Enrollment at All Blue Cross and Blue Shield Plans for Contract Years 2018-2019	3/12/21	5	1		
3	**Total Reports**		23	3	1	$1,227,289

Other Insurance Audits

Report Number	Name	Date	Total # of Recs.	# of Open Procedural Recs.	Monetary Findings	
					# Open	Amount
1H-07-00-19-017	CareFirst BlueChoice's Pharmacy Operations as Administered by CVS Caremark	7/20/2020	8	4	1	$834,425
4A-HI-00-19-007	Audit of the U.S. Office of Personnel Management's Administration of Federal Employee Insurance Programs	10/30/2020	24	13	0	$0
2	**Total Reports**		32	17	1	$834,425

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	4	0	$0
4K-ES-00-19-032	Presidential Rank Awards Program	1/17/2019	4	4	0	$0
4	**Total Reports**		16	10	0	$0

Management Advisories and Other Reports						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**Monetary Findings**	
					# Open	**Amount**
4K-RS-00-14-076	Review of OPM's Compliance with the Freedom of Information Act	3/23/2015	3	2	0	$0
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
4A-DO-00-20-041	Delegation of Authority to Operate and Maintain the Theordore Roosevelt Federal Building and the Federal Executive Institute	8/5/2020	4	3	0	$0
4	**Total Reports**		12	10	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