U.S. Office of Personnel Management

Office of the Inspector General

Open Recommendations

Open Recommendations Over Six Months Old as of March 31, 2023

June 1, 2023

Executive Summary

Open Recommendations Over Six Months Old as of March 31, 2023

June 1, 2023

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 Reform, 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.

Krista A. Boyd
Inspector General

As of March 31, 2023, there were 361 unimplemented recommendations, 215 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 03/31/2023	# Unique Recs. as of 03/31/2023
Internal Audits	28	258	154	75
IT Audits	35	615	138	71
Experience-Rated Insurance Audits	3	33	9	9
Community-Rated Insurance Audits	3	66	7	7
Other Insurance Audits	5	40	17	17
Evaluations	3	13	9	9
Management Advisories and Other Reports	6	31	27	27
Total	83	1,056	361	215

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	153	1	$6,140,755
IT Audits	138	0	0
Experience-Rated Insurance Audits	7	2	$811,277
Community-Rated Insurance Audits	5	2	$13,786,995
Other Insurance Audits	16	1	$834,425
Evaluations	9	0	0
Management Advisories and Other Reports	26	1	$164,212
Total	354	7	$21,737,664

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

Table of Contents

I. Internal Audits

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

[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	Open - unresolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

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	Open - unresolved
Rec. #2	***Finding***	Capitalizing on RSM Technology – A modernized environment offers opportunities to reduce instances of fraud, waste, and abuse of the retirement trust fund.
	Recommendation	The OIG recommends that OPM actively explore the capabilities of any automated solution to flag records and produce management reports for anomalies or suspect activity, such as multiple address or bank account changes in a short time.
	Status	Open - unresolved

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	Open - unresolved

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	Open - unresolved

* Represents Repeat Recommendations.

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	Open - unresolved

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	Open - unresolved
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	Open - unresolved
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.

* Represents Repeat Recommendations.

Continued: Audit of OPM's Fiscal Year 2014 Financial Statements		
Rec. #3 (cont.)	***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	Open - unresolved

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	Open - unresolved .
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	Open - unresolved
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.

Continued: Audit of OPM's Fiscal Year 2015 Financial Statements		
Rec. #3 (cont).	***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	Open - unresolved
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	Open - unresolved

Title: Audit of OPM's Office of Procurement Operations' Contract Management Process **Report #: 4A-CA-00-15-041** **Date: July 8, 2016**		
Rec. #2	***Finding***	Inaccurate Contract Amounts Reported in OPM's Information Systems - We requested access to 60 contract files with open obligations reported in the OCFO's CBIS Fiscal Years 2010 to 2014 Open Obligation Report and determined that the contract amounts reported in the Consolidated Business Information System (CBIS) for 22 of the 60 contracts sampled differed from the contract amounts reported in OPO's contract files. In addition, OPO was unable to provide 17 of the 60 contract files, so we cannot determine if the amounts reported in CBIS were accurate.
	Recommendation	The OIG recommends that OPO implement internal controls to ensure that contract data, including contract award amounts, is accurately recorded in OPM's information systems, such as CBIS, and the appropriate supporting documentation is maintained.
	Status	Open - unresolved
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	Open - unresolved

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	Open – unresolved

Title: Audit of OPM's Fiscal Year 2016 Financial Statements **Report #: 4A-CF-00-16-030** **Date: November 14, 2016**		
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	Open - unresolved
Rec. #3	***Finding***	Information Systems Control Environment: The FISMA Inventory Listing is incomplete.
	Recommendation	Grant Thornton recommends that OPM enhance processes in place to track the inventory of the Agency's systems and devices.
	Status	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Continued: Audit of OPM's Fiscal Year 2016 Financial Statements		
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	Open - unresolved
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	Open - unresolved
Rec. #10	***Finding***	Information Systems Control Environment: [redacted] are not PIV-compliant.
	Recommendation	Grant Thornton recommends that OPM implement two-factor authentication at the application level in accordance with agency and federal policies.
	Status	Open - unresolved
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	Open - unresolved
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	Open - unresolved
Rec. #14	***Finding***	Information Systems Control Environment: The FACES audit logs are not periodically reviewed.
	Recommendation	Grant Thornton recommends that OPM review audit logs on a pre-defined periodic basis for violations or suspicious activity and identify individuals responsible for follow-up or evaluation of issues to the Security Operations Team for review. The review of audit logs should be documented for record retention purposes.
	Status	Open - unresolved

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	Open - unresolved
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	Open - unresolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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

* Represents Repeat Recommendations.

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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	Open - unresolved

* 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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open – unresolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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	Open - unresolved
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	Open - unresolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Continued: Audit of OPM's 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	Open - unresolved

Title: Audit of OPM's Fiscal Year 2017 Improper Payments Reporting **Report #: 4A-CF-00-18-012** **Date: May 10, 2018**		
Rec. #2	***Finding***	The overall intent of the Improper Payments Information Act of 2002, as amended by IPERA and IPERIA, is to reduce improper payments. While Retirement Services met its improper payment reduction targets for fiscal years 2012 through 2017, Retirement Services' improper payments rate remained basically stagnant during that time period, at roughly an average of 0.37 percent. In addition, Retirement Services' improper payment amounts increased every year from 2012 to their current level of more than $313 million.
	Recommendation	The OIG recommends that Retirement Services develop and implement additional cost-effective corrective actions, aimed at the root cause(s) of improper payments, in order to further reduce the improper payments rate.
	Status	Open - unresolved

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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

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

* 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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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	Open - unresolved
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	Open - unresolved

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. #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	Open - unresolved

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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Audit of OPM's Fiscal Year 2019 Financial Statements		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* 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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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***	HI's 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 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	Open – resolved

* Represents Repeat Recommendations.

Continued: Audit of 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	Open – resolved
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	Open – resolved
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	Open - resolved
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 perform the Over Age 90 project of the annuitant population on a more routine basis, such as annually or biannually.
	Status	Open - resolved
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	Open - resolved
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	Open - resolved

Continued: Audit of 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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - resolved

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. #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	Open - unresolved

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	Open - resolved
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	Open - resolved
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	Open - resolved

* Represents Repeat Recommendations.

Continued: Audit of OPM'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	Open - resolved
Rec. #8	***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 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	Open - resolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Audit of OPM's Fiscal Year 2020 Financial Statements		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Title: Audit of the U.S. Office of Personnel Management's Fiscal Year 2020 Improper Payments Reporting **Report #: 4A-CF-00-21-008** **Date: May 17, 2021**		
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 IPERIA, and PIIA, which is to reduce improper payments, had not been met.
	Recommendation	We recommend that Retirement Services develop and implement additional cost-effective corrective actions, aimed at the root causes of improper payments, to further reduce the improper payments rate.
	Status	Open - unresolved

Title: Audit of OCIO's Revolving Fund Programs **Report #: 4A-CI-00-20-034** **Date: September 9, 2021 and reissued on November 22, 2021**		
Rec. #2	***Finding***	See #1 above.
	Recommendation	We recommend that the OCIO and the HCDMM strengthen internal controls to ensure that all inputs used in the HRS IT PMO and the eOPF office's pricing methodologies are properly reviewed, approved, documented, and properly maintained. Documentation should include but not be limited to detailed reports, calculations, and methodology, to ensure the data is valid, complete, and transparent.
	Status	Open - unresolved

Title: OPM's Compliance with DATA Act **Report #: 4A-CF-00-20-044** **Date: November 8, 2021**		
Rec. #3	***Finding***	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. Specifically, 23 out of 199 transactions tested were identified in File C (award financial) and not in File D1 (award procurement).
	Recommendation	We recommend that OPO work with the Contracting Officer Representatives to establish and implement management controls to ensure that contracts are tracked and managed through the closeout process and adequate documentation is maintained in the contract files, including evidence of contract completion and closeout.
	Status	Open - resolved

Title: Audit of OPM's Fiscal Year 2021 Financial Statements **Report #: 4A-CF-00-21-027** **Date: November 12, 2021**		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Continued: Audit of OPM's Fiscal Year 2021 Financial Statements		
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	Open - unresolved
Rec. #8*	***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	Open - unresolved
Rec. #9*	***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	Open - unresolved
Rec. #10*	***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	Open - unresolved
Rec. #11*	***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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Audit of OPM's Fiscal Year 2021 Financial Statements		
Rec. #12*	***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	Open - unresolved
Rec. #13*	***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	Open - unresolved
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 mechanism to systematically track all configuration items that are migrated to production in order to produce a complete and accurate listing of all configuration items. Further, develop, document, implement, and enforce requirements and processes to periodically validate that all configuration items migrated to production are authorized and valid.
	Status	Open - unresolved
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	Open - unresolved

Continued: Audit of OPM's Fiscal Year 2021 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	Open - unresolved
Rec. #20*	***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	Open - unresolved

Title: Audit of OPM's Utilization of the Improper Payments Do Not Pay Initiative **Report #: 4A-CF-00-20-029** **Date: February 14, 2022**		
Rec. #5	***Finding***	OPM's prescreening of new carriers' participation in the FEHBP has not included a review of the DNP Portal since 2017. In addition, Healthcare and Insurance does not have written policies and procedures for utilizing the DNP Portal in prescreening new carriers, because existing carriers have already been screened and awarded a contract.
	Recommendation	We recommend that Healthcare and Insurance always utilize Treasury's DNP Portal to verify carriers' eligibility before they are accepted into the FEHBP.
	Status	Open - resolved
Rec. #7	***Finding***	OPM should maintain an active relationship with the DNP Business Center to make the most of their analytic services and new data sources continually being added in the DNP Portal. OPM should ensure that they are aware of these new tools as they become available to determine if the new data sources would be beneficial to OPM's analytical endeavors.
	Recommendation	We recommend that OPM continue to work with the DNP Business Center to determine if OPM's program offices are targeting the best processes and data sources to meet their individual program needs of identifying improper payments.
	Status	Open - unresolved

Title: Audit of OPM's Compliance with the Payment Integrity Information Act Report #: 2022-IAG-002 Date: June 23, 2022		
Rec. #3*	***Finding***	Retirement Services did not meet its reduction target for FY 2021 and did not provide documentation supporting that OPM senior management determined the tolerable improper payment and unknown payment rate.
	Recommendation	We recommend that Retirement Services provide supporting documentation to substantiate that adjusting their FY 2021 reduction target further would be cost and mission prohibitive.
	Status	Open - unresolved
Rec. #6*	***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 IPERIA, and PIIA, which is to reduce improper payments, had not been met.
	Recommendation	We recommend that Retirement Services develop and implement additional cost-effective corrective actions, aimed at the root causes of improper payments, to further reduce the improper payments rate.
	Status	Open - unresolved

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	Open - unresolved

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	Open - unresolved

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	Open - unresolved

* Represents Repeat Recommendations.

[2] As defined in OMB Circular No. A-50, Open - 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 Open - resolved are not in compliance with the OMB Circular No. A-50 requirement that recommendations be Open - resolved within six months after the issuance of a final report.

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	Open - unresolved

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	Open - unresolved

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	Open - unresolved

Title: Federal Information Security Management Act Audit FY 2014 Report #: 4A-CI-00-14-016 Date: November 12, 2014		
Rec. #7	***Finding***	Configuration Management: 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
	Status	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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 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	Open - unresolved

* Represents Repeat Recommendations.

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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

* Represents Repeat Recommendations.

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

Title: Audit of OPM's Security Assessment and Authorization Report #: 4A-CI-00-17-014 Date: June 20, 2017		
Rec. #1	***Finding***	System Security Plan: The LAN/WAN SSP does not fully and accurately identify all of the security controls applicable to this system.
	Recommendation	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	Open - unresolved
Rec. #2	***Finding***	System Controls Assessment: The LAN/WAN security controls assessment likely did not identify vulnerabilities that could have been detected with a thorough test.
	Recommendation	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	Open - unresolved
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	Open - unresolved

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: 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	Open – resolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Continued: Audit of OPM's SharePoint Implementation		
Rec. #8	***Finding***	Patch Management: Vulnerability scans revealed several servers missing critical patches released more than 90 days before the scans took place. The OCIO responded that they were aware of the missing patches, but with no test environment to test the patches before being deployed into production SharePoint servers, the decision was made to not apply the critical patches.
	Recommendation	The OIG recommends that OPM implement a process to test patches on its SharePoint servers. Once this process has been implemented, we recommend OPM implement controls to ensure all critical patches are installed on SharePoint servers and databases in a timely manner as defined by OPM policies.
	Status	Open - unresolved

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

* Represents Repeat Recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2017		
Rec. #28	***Finding***	ICAM Strategy: OPM has not developed an ICAM strategy that includes a review of current practices ("as-is" assessment), identification of gaps (from a desired or "to-be" state), and a transition plan.
	Recommendation	The OIG recommends that OPM develop and implement an ICAM strategy that considers a review of current practices ("as-is" assessment) and the identification of gaps (from a desired or "to-be" state) and contains milestones for how the agency plans to align with Federal ICAM initiatives.
	Status	Open - unresolved
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	Open – unresolved
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	Open – unresolved

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	Open - unresolved

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	Open - unresolved
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	Open - unresolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2018		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2018		
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	Open – unresolved
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	Open – unresolved
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	Open – unresolved

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	Open – resolved

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	Open - resolved

* Represents Repeat Recommendations.

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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.

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. #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	Open – unresolved

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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
Rec. #11	***Finding***	Privacy Impact Assessment - ESI & LAN/WAN General Support Systems: In the most recent Authorizations, the ESI GSS's PTA was not complete (i.e., it did not indicate whether a PIA is required) or approved and the LAN/WAN GSS package did not include a PTA. PIAs for both GSSs were not provided during the course of the audit.
	Recommendation	We recommend that OPM complete and approve a PTA and PIA (if required by the PTA) for the LAN/WAN GSS in accordance with the requirements of the E-Government Act of 2002 and OPM policy.
	Status	Open - unresolved

Continued: Audit of OPM's Compliance with the Data Center Optimization Initiative		
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	Open - unresolved
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	Open – unresolved
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	Open - unresolved

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

* Represents Repeat Recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2019		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Continued: Federal Information Security Modernization Act Audit FY 2019		
Rec. #29*	***Finding***	ICAM Strategy: In FY 2017, it was determined OPM has not developed and implemented an ICAM strategy containing milestones for how the agency plans to align with Federal ICAM initiatives. As noted above, OPM had not considered ICAM to be a distinct program and thus there were no corrective actions in FY 2018 or FY 2019.
	Recommendation	We recommend that OPM develop and implement an ICAM strategy that considers a review of current practices ("as-is" assessment) and the identification of gaps (from a desired or "to-be" state), and contains milestones for how the agency plans to align with Federal ICAM initiatives.
	Status	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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. #3	***Finding***	Contingency Plan Testing: 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	Open - unresolved

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. #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 HVAs. 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	Open - unresolved
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 SO, the CISO, the 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	Open - unresolved
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 ISSOs.
	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	Open - unresolved

Continued: Audit of OPM'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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

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 30, 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	Open - unresolved
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	Open - unresolved
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	Open – unresolved

Title: Federal Information Security Management Act Audit FY 2020 **Report #: 4A-CI-00-20-010** **Date: October 30, 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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Continued: Federal Information Security Modernization Act Audit FY 2020		
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved
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	Open - unresolved

Continued: Federal Information Security Modernization Act Audit FY 2020		
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	Open - unresolved
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	Open – unresolved
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	Open – unresolved
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	Open – unresolved
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	Open – unresolved

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. #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	Open – resolved
Rec. #12	***Finding***	Security Configuration Auditing: [redacted]
	Recommendation	We recommend that BSWH [redacted]
	Status	Open - resolved

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: 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	Open - resolved

Title: Audit of the Information Systems General and Application Controls at SelectHealth **Report #: 1C-SF-00-21-005** **Date: September 13, 2021**		
Rec. #1	***Finding***	Security Management - Entity Segmentation: [redacted] Without the use of a [redacted] presents the risk [redacted].
	Recommendation	We recommend that SelectHealth implement firewall protection between its sensitive resources and network connections with IMH.
	Status	Open - resolved
Rec. #6	***Finding***	Network Security - Internal Network Segmentation: [redacted]
	Recommendation	We recommend that SelectHealth [redacted]
	Status	Open - resolved

Title: Audit of the Information Technology Controls of the U.S. Office of Personnel Management's Executive Schedule C System **Report #: 4A-ES-00-21-020** **Date: September 30, 2021**		
Rec. #10	***Finding***	NIST SP 800-53 Controls Testing - System Inventory: The ESCS does not have a system-level configuration management plan to identify and manage configuration items throughout the system development lifecycle.
	Recommendation	We recommend that OPM develop a system-level configuration management plan for the ESCS that establishes a process for identifying and managing configuration items and documentation.
	Status	Open - unresolved

Title: Federal Information Security Modernization Act Audit - Fiscal Year 2021 **Report #: 4A-CI-00-21-012** **Date: October 27, 2021**		
Rec. #2*	***Finding***	Software Inventory: Although OPM has mechanisms in place to capture some software information, policies and procedures for developing and maintaining an up-to-date software inventory have not been developed.
	Recommendation	We recommend that OPM define policies and procedures for a centralized software inventory.
	Status	Open - unresolved

* Represents Repeat Recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2021		
Rec. #7*	***Finding***	Metric 6 - Information Security Architecture: A Security Reference Model has yet to be established in the current Enterprise Architecture document.
	Recommendation	We recommend that OPM update its enterprise architecture, to include the information security architecture elements required by NIST and OMB guidance.
	Status	Open - unresolved
Rec. #11*	***Finding***	Metric 12 - SCRM Strategy: Further, OPM did not provide any evidence for the metric to demonstrate achievement of a maturity level. Therefore, the default maturity level for the metric is Ad Hoc. The following recommendation is to assist OPM with attaining the Defined maturity level.
	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	Open - unresolved
Rec. #13*	***Finding***	Metric 18 - Configuration Management Plan: OPM has developed a CM plan that outlines CM-related roles and responsibilities, institutes a change control board, and defines processes for implementing configuration changes; however, the agency has not integrated its overall configuration management plan into its continuous monitoring and risk management programs. OPM has also 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	Open - unresolved
Rec. #14*	***Finding***	Metric 19 - 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	Open - unresolved
Rec. #15*	***Finding***	Metric 20 - 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 Defense Information Systems Agency's Security Technical Implementation 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	Open – unresolved
Rec. #16*	***Finding***	Metric 20 - 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 Defense Information Systems Agency's Security Technical Implementation 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	Open – unresolved

* Represents Repeat Recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2021		
Rec. #17	***Finding***	Metric 21 - Flaw Remediation and Patch Management: After reviewing the results, we identified approximately 30 critical or high findings that were past their 30-day remediation deadline.
	Recommendation	We recommend that the OCIO implement a process to apply critical operating system and third- party vendor patches in a 30-day window according to OPM policy.
	Status	Open – unresolved
Rec. #18*	***Finding***	Metric 21 - Flaw Remediation and Patch Management: We also determined that there is no 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	Open – unresolved
Rec. #19	***Finding***	Metric 22 - Trusted Internet Connection Program: In FY 2021, OPM did not provide any evidence to demonstrate that the controls for this metric improved or are still in place.
	Recommendation	We recommend that OPM establish an agency-wide TIC program to manage and maintain its external agency connections.
	Status	Open – unresolved
Rec. #20	***Finding***	Metric 26 - ICAM Roles, Responsibilities, and Resources: OPM has not developed an ICAM governance structure to align and consolidate the agency's ICAM investments, monitor programs, and ensure awareness and understanding. Roles and responsibilities for all users should be incorporated in a comprehensive ICAM strategy.
	Recommendation	We recommend that OPM create a charter to govern the roles and responsibilities of its ICAM office's governance body.
	Status	Open – unresolved
Rec. #21*	***Finding***	Metric 27 - ICAM Strategy: OPM has not developed these or a plan to meet the requirement.
	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	Open – unresolved
Rec. #22	***Finding***	Metric 32 - Management of Privileged User Accounts: OPM has not defined its process for provisioning, managing, and reviewing privileged accounts. Defined processes should cover approval and tracking, inventorying, validating, and logging and reviewing privileged users' accounts.
	Recommendation	We recommend that OPM define its process for provisioning, managing, and reviewing privileged accounts.
	Status	Open - unresolved
Rec. #27*	***Finding***	Metric 38 - Data Breach Response Plan: 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	Open - unresolved

* Represents Repeat Recommendations.

Continued: Federal Information Security Modernization Act Audit FY 2021		
Rec. #28*	***Finding***	Metric 39 - Privacy Awareness Training: OPM has not defined its privacy awareness training program based on the organizational requirements, culture, and the types of PII that its users have access to. In addition, the organization has not developed role-based privacy training for individuals having responsibility for PII or activities involving PII.
	Recommendation	We recommend that OPM identify individuals with heightened responsibility for PII and provide role-based training to these individuals at least annually.
	Status	Open - unresolved
Rec. #32*	***Finding***	Metric 60 - Contingency Planning Roles and Responsibilities: While OPM is making progress, we continue to see a lapse in contingency plan maintenance and testing leading to updates performed in an ad hoc manner.
	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	Open - unresolved
Rec. #34*	***Finding***	Metric 62 - Contingency Plan Maintenance: OPM has not updated system-level contingency plans annually.
	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	Open - unresolved
Rec. #35*	***Finding***	Metric 63 - Contingency Plan Testing: Like last year, OPM has not effectively performed annual contingency plan testing for all systems within its inventory.
	Recommendation	We recommend that OPM test the contingency plans for each system on an annual basis.
	Status	Open - unresolved
Rec. #36*	***Finding***	Metric 64 - Information System Backup and Storage: However, we did not observe any evidence 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.
	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	Open – unresolved

Title: Audit of the Information Systems General and Application Controls at EmblemHealth Report #: 1D-80-00-21-025 Date: March 21, 2022		
Rec. #2	***Finding***	Vulnerabilities Identified by OIG Scans: EmblemHealth is unable to quickly remediate these vulnerabilities on legacy systems with application dependencies. EmblemHealth has ongoing projects to decommission these legacy systems.
	Recommendation	We recommend that EmblemHealth remediate the specific technical weaknesses discovered during this audit as outlined in the vulnerability scan audit inquiry.
	Status	Open - resolved
Rec. #5	***Finding***	System Lifecycle Management: EmblemHealth was aware of the unsupported software and tracks those instances. The challenge to removing the unsupported software is the need for legacy systems to be available during a period of transition to new systems. EmblemHealth indicated that several projects are in place to migrate away from legacy applications by 2022.
	Recommendation	We recommend that EmblemHealth develop and implement action plans to upgrade or decommission the unsupported software identified during this audit.
	Status	Open - resolved

Title: Audit of the Information Systems General and Application Controls at Blue Cross and Blue Shield of Alabama Report #: 2022-ISAG-006 Date: August 22, 2022		
Rec. #1	***Finding***	Risk Response: During our audit, we found that BCBSAL [redacted]. In response to this finding, BCBSAL [redacted]
	Recommendation	We recommend that BCBSAL formally [redacted]
	Status	Open – resolved

III. Experience-Rated Health Insurance Audits

This section describes the open recommendations from audits of experience-rated health insurance carriers that participate in the Federal Employees Health Benefits Program (FEHBP).[3]

Title: Audit of Claims Processing and Payment Operations at Health Care Service Corporation for Contract Years 2018 through 2020 **Report #: 1A-10-17-21-018** **Original Issue Date: February 23, 2022** **Corrected Issue Date: Reissued March 16, 2022**		
Rec. #13	***Finding***	Proactive Notification to Members: BCBSA (Association) does not proactively identify enrollees that previously utilized a newly debarred provider and notify them of the provider's debarment status as required by the Federal regulations and OPM OIG's Guidelines for Implementation of FEHBP Debarment and Suspension Orders (Guidelines).
	Recommendation	We recommend that the contracting officer direct the Association to update its debarment procedures to include the Guidelines' proactive notification requirements.
	Status	Open - unresolved
Rec. #14	***Finding***	Incomplete Enrollee Notification: The Association's enrollee notification of a provider's debarment status on the Explanation of Benefits (EOB) does not include all the required information to be communicated to the enrollee. Additionally, notification via the EOB is not the clearest way to communicate this type of important information to enrollees.
	Recommendation	We recommend that the contracting officer direct the Association to include all required enrollee notifications as stated in the Guidelines in the messaging to enrollees for debarred providers.
	Status	Open - unresolved
Rec. #15	***Finding***	Notification to the OIG: The Association does not notify the OIG of debarred providers who submit claims for services following the effective date of their debarments. Additionally, the Association's SAR to the OIG, which occasionally includes a listing of debarred claims paid by providers, appears to be incomplete.
	Recommendation	We recommend that the contracting officer direct the Association to notify OIG monthly of all claims submitted by debarred providers after the effective date of their debarments.
	Status	Open - unresolved

[3] As defined in OMB Circular No. A-50, Open - 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 Open - resolved are not in compliance with the OMB Circular No. A-50 requirement that recommendations be Open - resolved within six months after the issuance of a final report.

Continued: Audit of Claims Processing and Payment Operations at Health Care Service Corporation		
Rec. #16	***Finding***	Notification to the OIG: The Association does not notify the OIG of debarred providers who submit claims for services following the effective date of their debarments. Additionally, the Association's SAR to the OIG, which occasionally includes a listing of debarred claims paid by providers, appears to be incomplete.
	Recommendation	We recommend that the contracting officer direct the Association to review its reporting practices to ensure that all claims paid to debarred providers are reported to the OIG on its SAR.
	Status	Open - unresolved

Title: Audit of Claims Processing and Payment Operations at Mail Handlers Benefit Plan for Contract Years 2019 through 2020 **Report #: 1B-45-00-21-034** **Issue Date: August 16, 2022**		
Rec. #1	***Finding***	Incorrect Non-Network Drug Allowance Applied: The Mail Handlers Benefit Plan (Plan) overcharged the FEHBP $565,197 for 626 claim lines that were not paid in accordance with the allowance as defined in Section 10 of the Plan's benefit brochure.
	Recommendation	We recommend that the contracting officer direct the Plan to disallow $565,197 in overcharges to the FEHBP resulting from this claim system error.
	Status	Open – unresolved
Rec. #2	***Finding***	Incorrect Non-Network Drug Allowance Applied: The Mail Handlers Benefit Plan (Plan) overcharged the FEHBP $565,197 for 626 claim lines that were not paid in accordance with the allowance as defined in Section 10 of the Plan's benefit brochure.
	Recommendation	We recommend that the contracting officer ensure that the Plan continues its efforts to identify all claims paid incorrectly due to this error and initiate recovery of all FEHBP overpayments.
	Status	Open - unresolved
Rec. #4	***Finding***	Debarred Claims Notification Process: The Plan did not have procedures in place to notify the OPM OIG when claims are submitted by providers debarred from the FEHBP after the effective date of their debarment, as required by the OPM OIG's Guidelines.
	Recommendation	We recommend that the contracting officer verify that the Plan's corrective action plan is in place and that it has begun to notify the OPM OIG when claims from debarred providers incurred after the effective date of debarment are submitted to it.
	Status	Open - unresolved

Title: Audit of BlueCross BlueShield of Tennessee **Report #: 1A-10-15-21-023** **Date: August 25, 2022**		
Rec. #1	***Finding***	Claim Overpayment Write-offs: BlueCross BlueShield of Tennessee (Plan) was not diligent in its efforts to recover $607,204 in Federal Employee Program (FEP) claim overpayments. These claim overpayments were originally set up as auto-recoupments (provider offsets), where the Plan would reduce future benefit payments to the providers for the purpose of recovering the refunds related to the overpayments but were then subsequently written off by the Plan. We noted that these FEP claim overpayments were outstanding from approximately 7 to 13 years. Based on Contract CS 1039, the Plan must make a prompt and diligent effort to recover an erroneous health benefit payment until the debt is paid in full or determined to be uncollectible. Unless the Plan provides support that these claim overpayments were uncollectible, we can only conclude that the Plan did not make diligent efforts to recover these funds before writing them off.
	Recommendation	We recommend that the contracting officer require the Plan to return $607,204 to the FEHBP for the claim overpayments that were written off by the Plan without adequate support and/or justification, whether recovered or not, as diligent efforts to recover were not made.
	Status	Open - unresolved
Rec. #3	***Finding***	Claim Overpayment Write-offs: The Association approved two special plan invoices, totaling $1,494,447, for Plan claim overpayment write-offs in October 2018. However, we could not determine if the Association verified that the Plan followed the applicable steps for due diligence in Section 2.3(g) of Contract CS 1039, before approving these write-offs. Although most of these write-offs were for claim overpayments less than $10,000, we noted that all our questioned claim overpayment write-offs were included in these two special plan invoices.
	Recommendation	We recommend that the contracting officer require the Association to implement corrective actions to ensure that the BCBS plans have followed proper overpayment recovery steps and demonstrated diligent recovery efforts, as required by Section 2.3(g) of Contract CS 1039, before the Association approves the plans' claim overpayment write-offs.
	Status	Open - unresolved

IV. Community-Rated Health Insurance Audits

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

Title: Audit of UPMC Health Plan, Inc. **Report #: 1C-8W-00-20-017** **Date: June 28, 2021**		
Rec. #1	***Finding***	During the 2014 through 2016 contract years, the Plan submitted premium rates for the FEHBP with High, Standard, and HDHP benefit options; however, we identified several defective pricing issues that resulted in lower audited premium rates for each option
	Recommendation	We recommend that the Plan return $12,174,183 to the FEHBP for defective pricing in contract years 2014 through 2016.
	Status	Open. ARC is still working to resolve the findings identified throughout the report to determine a final defective pricing amount.
Rec. #2	***Finding***	The Plan erroneously included a loading in the 2014 through 2016 premium rates to account for the Health Insurance Providers Fee (HIF) established under the Patient Protection and Affordable Care Act (ACA), Section 9010.
	Recommendation	We recommend that the Plan remove all HIF loadings from the FEHBP premium rate developments and MLR filing denominators (as applicable) that have been submitted to OPM under Contract CS 2856.
	Status	Open - unresolved
Rec. #10	***Finding***	In accordance with the FEHBP regulations and the contract between OPM and the Plan, the FEHBP is entitled to recover Lost Investment Income (LII) on the defective pricing finding in contract years 2014 through 2016.
	Recommendation	We recommend that the Plan return $1,612,812 to the FEHBP for LII, calculated through May 31, 2021. We also recommend that the Plan return LII on amounts due for the period beginning June 1, 2021, until all defective pricing finding amounts have been returned to the FEHBP.
	Status	Open - unresolved
Rec. #11	***Finding***	The Plan calculated unadjusted MLRs of 93.58 percent, 93.15 percent, and 88.33 percent for contract years 2014, 2015, and 2016 respectively. Since contract years 2014 and 2015 ratios exceeded the OPM established threshold of 89 percent, the Plan received OPM credits of $3,370,927 and $3,170,143 respectively. However, during our review of the FEHBP MLR filings, we adjusted the MLR denominators in each audit scope year to reflect the defective pricing discussed in section A.1. of this report, as shown below in Table V.
	Recommendation	We recommend that the Contracting Officer adjust the Plan's MLR credit for contract years 2014 through 2016 once the defective pricing findings discussed in this report are Open - resolved.
	Status	Open – unresolved

Title: Audit of Independent Health Association, Inc. Report #: 1C-QA-00-21-003 Date: January 7, 2022		
Rec. #8	***Finding***	The Certificates of Accurate MLR signed by the Plan for contract years 2016 through 2018 were defective. All penalty adjustments will be calculated by OPM after the defective pricing findings are resolved and collected. Any adjustments to the defective pricing findings in this report may also impact the credit reductions. The specific issues that led to the penalty adjustments and defective Certificates of Accurate MLR are discussed throughout the remainder of the report.
	Recommendation	We recommend that the Contracting Officer adjust the Plan's MLR credits for contract years 2016 through 2018 once the defective pricing findings discussed in this report are resolved.
	Status	Open - unresolved

Rec. #30	***Finding***	As discussed in Section A of this draft report, our audit identified defective pricing findings related to the Plan's premium rates in contract years 2016 through 2018, totaling $1,079,748. The Community Rating Guidelines state that the denominator of the FEHBP MLR calculation will be equal to the OPM supplied premium income or carrier supplied premium income less any amount recovered from the carrier due to an audit.
	Recommendation	We recommend the Contracting Officer reduce the 2016 through 2018 MLR premiums by $730,246 in 2016, $224,314 in 2017, and $125,188 in 2018 for the questioned premium costs identified in this audit.
	Status	Open - unresolved

Title: Audit of Kaiser Foundation Health Plan Report #: 1C-59-00-20-043 Date: August 16, 2022		
Rec. #1	***Finding***	Throughout our review of Kaiser Foundation Health Plan's (Plan) FEHBP Medical Loss Ratio (MLR), it was apparent that due to the Plan's integrated health care system, which provides both medical care and coverage, compliance with the reporting requirements was and is in many cases unattainable. FEHBP carriers with integrated health systems like the Plan, including other carriers with complicated corporate structures, are fundamentally unable to meet the reporting requirements that the FEHBP MLR requires of them. This represents a huge time and monetary burden that is placed on carriers, which, based on the OIG's audits of the application of the MLR process by a number of FEHBP carriers over the last several years, results in an unreliable FEHBP MLR that should not be used by OPM to ascertain that the Government and Federal employees are receiving a fair market rate and a good value for their premium dollars.
	Recommendation	We recommend that OPM revise or replace the FEHBP MLR requirements to provide a reliable measure of the premium dollars spent on the FEHBP program, including the impact of carrier corporate structure and the current community-rated product market.
	Status	Open - unresolved

V. Other Insurance Audits

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

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 - unresolved
Rec. #2	***Finding***	See Rec. #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 - unresolved

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 for retail pharmacy claims with Walgreens and Rite Aid retail pharmacy claims for CYs 2014 through 2016.
	Status	Open - unresolved.

Continued: Audit of Carefirst BlueChoice FEHBP Pharmacy Operations as Administered by CVS Caremark		
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	Open - unresolved.
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	Open - unresolved.

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. #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	Open - unresolved.
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	Open - resolved.

Continued: Audit of the U.S. Office of Personnel Management's Administration of Federal Employee Insurance Programs		
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	Open - unresolved.
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	Open - unresolved.
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	Open - unresolved.
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	Open - unresolved.
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	Open - unresolved.

Title: Audit of the Reasonableness of Selected FEHBP Carrier's Pharmacy Benefit Contracts Report #: 1H-99-00-20-016 Date: July 29, 2021		
Rec. #1	***Finding***	Pooling of Carrier Contracts: Based on discussions with the PBM and our overall review of each carrier's expenses related to the PBM's administration of pharmacy benefits, we believe it would lower FEHBP pharmacy costs if the carriers pooled their resources in a common PBM agreement.
	Recommendation	We recommend that the Contracting Office direct its carriers to consider pooling their resources into a common PBM agreement, which could potentially not only lower costs to the program but also to its federal members.
	Status	Open - unresolved
Rec. #2	***Finding***	Inappropriate Application of Transparency Standards: Our review of claims from the five nation-wide Carriers found that the PBM's contracting practices with the carriers and pricing and payment of retail pharmacy claims do not appear to meet the PBM transparency standards as established by OPM in 2011.
	Recommendation	We recommend that the Contracting Officer complete a data analysis of the claims pricing for all FEHBP carriers who contract with the PBM to determine if the transparency standards are being implemented as intended.
	Status	Open - unresolved
Rec. #3	***Finding***	Inappropriate Application of Transparency Standards: Our review of claims from the five nation-wide Carriers found that the PBM's contracting practices with the carriers and pricing and payment of retail pharmacy claims do not appear to meet the PBM transparency standards as established by OPM in 2011.
	Recommendation	We recommend that the Contracting Officer require the carrier contracts to include a true-up to ensure that each carrier receives the full value of all discounts, rebates, credits, or any other financial guarantees or adjustments included within the PBM's contracts with pharmacies. The true-ups should ensure that only the final costs paid to the pharmacies and/or drug suppliers (including any post point of sale reconciliations or true-ups) are passed on to the FEHBP.
	Status	Open - unresolved

Title: Audit of the Federal Long Term Care Insurance Program Report #: 1G-LT-00-21-013 Date: September 12, 2022		
Rec. #2	***Finding***	Our audit identified one program improvement area for the administration of the FLTCIP. Specifically, we determined that the Contractor and OPM need to strengthen their procedures and controls related to the FLTCIP funding status and the frequency of setting premium rates.
	Recommendation	We recommend that OPM instruct the Contractor to immediately notify FLTCIP subscribers of the change in funding level assumptions, and any corrective actions being considered to properly fund the program, so that participants have adequate time to plan for premium increases and/or benefit reductions.
	Status	Open - unresolved.
Rec. #3	***Finding***	See Rec. #2 above.
	Recommendation	We recommend that OPM work with the Contractor to develop an annual communications plan to provide summary level FLTCIP funding status to participants, so they are properly informed of the program's funding level.
	Status	Open - unresolved.

VI. 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 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	Open - unresolved

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	Open – unresolved
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	Open – unresolved

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	Open - unresolved
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	Open - unresolved

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 update and finalize its standard operating procedures to ensure its staff document required responsibilities.
	Status	Open – unresolved
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	Open - unresolved

Continued: Evaluation of the Presidential Rank Awards Program		
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	Open – unresolved
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	Open - unresolved

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	Open - resolved
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	Open - resolved

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	Open - unresolved
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	Open - unresolved

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	Open - unresolved

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	Open - unresolved
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	Open - unresolved

Title: FEHB Program Integrity Risks Due to Contractual Vulnerabilities **Report #: 4A-HI-00-18-026** **Date: April 1, 2021**		
Rec. #1	***Finding***	Data Retention Periods: The FEHBP contract's current records retention clause requires the retainment of records for a period of six years after the end of the contract term to which the records relate. However, OIG's Office of Investigations' (OI) False Claims Act (FCA) investigations have a 10-year statute of limitations, requiring the need for subpoenas to obtain any information beyond the FEHBP contract's six-year requirement.
	Recommendation	We recommend that OPM modify FEHBP contract language for all applicable records retention clauses to require the retention and accessibility of claims for 10 years plus the current year in a manner of OPM/HI's choosing.
	Status	Open – unresolved
Rec. #2	***Finding***	Strengthening Language in Contract Section 1.9(a) Related to Fraud, Waste, and Abuse: The broad nature of this clause makes it unclear whether or not OPM issued Carrier Letters (CLs) are binding as part of the contract.
	Recommendation	We recommend OPM modify or add language in Section 1.9 of all FEHBP contracts to include all relevant sections and attachments of CL 2017-13 or modify all FEHBP contracts to add relevant language stating that all CLs are an addendum to the contract language and enforceable as a contract requirement.
	Status	Open - unresolved
Rec. #3	***Finding***	Fraud and Abuse Recoveries: Section 1.9 of the FEHBP contracts does not provide instructions to carriers as to where to return the fraud-related recoveries reported in carriers' annual fraud reports. Instead, these funds are often treated as erroneous payments and returned or credited to the Letter of Credit Account, which means they cannot be used to benefit enrollees by mitigating potential premium increases.
	Recommendation	We recommend OPM modify or add language to the appropriate Section of the fee-for-service and experience-rate HMO contracts to state that all Fraud, Waste, and Abuse-related recoveries must be deposited into the working capital or investment account within 30 days and returned to or accounted for in the FEHBP contingency reserve fund account within 60 days after receipt by the carrier.
	Status	Open - unresolved

Continued: FEHB Program Integrity Risks Due to Contractual Vulnerabilities		
Rec. #4	***Finding***	Protecting the Integrity of OIG Investigations: Conflicts can emerge when carriers proceed with internal fraud investigative activities without awareness or regard to ongoing OIG investigations.
	Recommendation	We recommend that OPM add language to all FEHBP contracts requiring carriers to notify the OIG's OI regarding their intention to share FEHBP fraudulent activity with outside parties and obtain approval from OIG's OI before sharing this information.
	Status	Open - unresolved
Rec. #5	***Finding***	Adding Language to FEHBP Contracts Requiring All Vendors and Large Provider Agreements to Adhere to OPM Anti-Fraud Requirements: The current FEHBP contract does not require all vendors and large providers to have a Fraud, Waste, and Abuse program in place, as is required for carriers under Section 1.9(a) and by CL 2017-13.
	Recommendation	We recommend that OPM modify or add language to all fee-for-service and experience-rated HMO FEHBP contracts requiring PBMs or providers under a Large Provider Agreement, who provide services or supplies related to benefit administration, to have a Fraud, Waste, and Abuse program that meets the OPM contract and CL 2017-13 requirements.
	Status	Open - unresolved
Rec. #6	***Finding***	Adding Language to FEHBP Contracts Requiring All Vendors and Large Provider Agreements to Adhere to OPM Anti-Fraud Requirements: The current FEHBP contract does not require all vendors and large providers to have a Fraud, Waste, and Abuse program in place, as is required for carriers under Section 1.9(a) and by CL 2017-13.
	Recommendation	We recommend that OPM modify the experience-rated HMO and fee-for-service contracts to require that vendors under Large Provider Agreements return all Fraud, Waste, and Abuse-related recoveries to the carrier within 30 days, whereby carriers must deposit these recoveries into their working-capital or investment account within 30 days. Once deposited into one of these accounts, the carrier must return the recoveries to the contingency reserve fund.
	Status	Open - unresolved

Continued: FEHB Program Integrity Risks Due to Contractual Vulnerabilities		
Rec. #7	***Finding***	The Erroneous Payments Clause: Contract Section 2.3(g) Erroneous Payments, as written, is too broad, does not give any type of routine recovery reporting, and may be costing the program for recovery efforts that could be handled in a more efficient manner.
	Recommendation	We recommend that OPM modify Section 2.3(g) and 2.3(g)(ii) to provide explanations for how carriers are to proactively identify overpayments and to define what it means by egregious errors.
	Status	Open - unresolved
Rec. #8	***Finding***	The Erroneous Payments Clause: Contract Section 2.3(g) Erroneous Payments, as written, is too broad, does not give any type of routine recovery reporting, and may be costing the program for recovery efforts that could be handled in a more efficient manner.
	Recommendation	We recommend that OPM modify Section 2.3(g) requiring carriers to report on their collection efforts, including how promptly the carrier initiated collection once the erroneous payment was identified and the causes of the claim payment errors.
	Status	Open - unresolved
Rec. #9	***Finding***	The Erroneous Payments Clause: Contract Section 2.3(g) Erroneous Payments, as written, is too broad, does not give any type of routine recovery reporting, and may be costing the program for recovery efforts that could be handled in a more efficient manner.
	Recommendation	We recommend that OPM review the current recovery process in Section 2.3(g)(1) through (5) and consider whether the use of benefit offsets, after the first written notification is sent, would be more cost effective.
	Status	Open - unresolved
Rec. #10	***Finding***	Use of Statistical Sampling: Use of statistical sampling is not currently included in FEHB carrier contracts, impeding our ability to use this widely accepted methodology to help identify erroneously paid claims.
	Recommendation	We recommend that OPM modify FEHBP contracts to clarify the Agency's authority to recoup projected improper payments identified by statistical sampling.
	Status	Open - unresolved

Continued: FEHB Program Integrity Risks Due to Contractual Vulnerabilities		
Rec. #11	***Finding***	Other Adjustments to Contract Clauses: Section 2.6(g) in the amendment to the Coordination of Benefits section of the fee-for-service contract currently precludes OPM from seeking reimbursement on low dollar claims under $100 and claims that are under $50 where Medicare is the primary payer of benefits that are tied to identified claims system errors.
	Recommendation	We recommend modifying Section 2.6(g) in the amendment to the Coordination of Benefits section of the fee-for-service contract, to allow for the recovery of low dollar claims that result from claims system errors.
	Status	Open - unresolved

Title: Review of the 2017 Presidential Management Fellows Program Application Process Redesign **Date: May 18, 2022**		
Rec. #1	***Finding***	OPM requested various aspects of the 2017 PMF application redesign be reviewed by our office; as such, we determined that the PMF Program did not perform the required functions to ensure program effectiveness and systemic program barrier identification. Although OPM noted that immediate modifications and long-term studies are being conducted for future PMF application cycles, the OIG made 8 recommendations to improve the process.
	Recommendation	The PMF Program should utilize applicant flow data to conduct organizational analyses in compliance with program regulations and develop robust policies. and procedures for this process. The results of this work should be made publicly available.
	Status	Open – unresolved
Rec. #2	***Finding***	See above
	Recommendation	The PMF Program Director and program leaders should maintain demographic analyses on a shared network drive in order to establish and promote cognitive awareness amongst PMF team members and develop policies and procedures surrounding this practice.
	Status	Open – unresolved
Rec. #3	***Finding***	See above
	Recommendation	The PMF Program should revise any current program documents (such as OPM CENTRAL-11) that lack clear and concise language surrounding the collection and use of applicant flow data.
	Status	Open – unresolved
Rec. #4	***Finding***	See above
	Recommendation	The PMF Program should implement proper controls to ensure complete and accurate applicant flow data is maintained should there be a system migration/update and develop policies and procedures surrounding this process.
	Status	Open – unresolved

Continued: Review of the 2017 Presidential Management Fellows Program Application Process Redesign		
Rec. #5	***Finding***	See above
	Recommendation	The PMF Program Director should immediately establish formal diversity and inclusion goals that align with agency guidance and Federal regulations and distribute official guidance on how these goals will be communicated, reviewed, modified, and approved on an annual basis to program staff.
	Status	Open – unresolved
Rec. #6	***Finding***	See above
	Recommendation	The PMF Program should continue to seek guidance from OPM's Office of Diversity, Equity, Inclusion, and Accessibility (ODEIA) to help memorialize concrete strategies and best practices surrounding Diversity, Equity, Inclusion, and Accessibility initiatives within the PMF Program.
	Status	Open – unresolved
Rec. #7	***Finding***	See above
	Recommendation	The PMF Program should develop and implement written policies and procedures surrounding the development of the assessment tools for every application cycle. If no assessment revisions occurred, it should be noted as such. Additionally, the Program should incorporate written procedures surrounding the reasons for assessment changes and the approval process for those changes.
	Status	Open – unresolved
Rec. # 8	***Finding***	See above
	Recommendation	The PMF Program should initiate annual internal audits/reviews of program statistics to assess the overall performance of the PMF Program. This review could include the number of participating agencies, demographic make-up of applicants and finalists, and the number of appointed Fellows.
	Status	Open – unresolved

Appendix

Below is a chart listing all reports described in this document that, as of March 31, 2023, had open recommendations over six months old.

Internal Audits						
			Total # of Recs.	# of Open Procedural Recs.	Monetary Findings	
Report Number	Name	Date			# 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-CA-00-15-041	OPM's OPO's Contract Management Process	07/08/2016	6	2	1	$6,140,755
4A-CF-00-16-030	FY 2016 Financial Statements	11/14/2016	19	12	0	$0
4A-CF-00-17-028	FY 2017 Financial Statements	11/13/2017	18	13	0	$0
4A-CF-00-15-049	OPM's Travel Card Program	01/16/2018	21	15	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	15	0	$0
4A-CF-00-19-012	FY 2018 IPERA	6/3/2019	4	1	0	$0
4A-CF-00-19-022	FY 2019 Financial Statements	11/18/2019	20	16	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	1	0	$0
4A-RS-00-19-038	Retirement Services Disability Process	10/30/2020	8	5	0	$0
4A-CF-00-20-024	FY 2020 Financial Statements	11/13/2020	21	16	0	$0
4A-CF-00-21-008	FY 2020 Improper Payments Reporting	5/17/2021	4	1	0	$0

Internal Audits						
			Total # of Recs.	# of Open Procedural Recs.	Monetary Findings	
Report Number	Name	Date			# Open	Amount
4A-CI-00-20-034	OCIO's Revolving Fund Programs	9/9/2021 and 11/22/2021	4	1	0	$0
4A-CF-00-20-044	OPM's Compliance with DATA Act	11/8/2021	3	1	0	$0
4A-CF-00-21-027	FY 2021 Financial Statements	11/12/2021	20	15	0	$0
4A-CF-00-20-029	OPM's Improper Payments Do Not Pay	2/14/2022	7	2	0	$0
2022-IAG-002	OPM's Compliance with the Payment Integrity Information Act	6/23/2022	6	2	0	$0
28	Total Reports		258	153	1	$6,140,755

Information Systems Audits						
			Total # of Recs	# of Open Procedural Findings	Monetary Findings	
Report Number	Name	Date			# 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	1	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	2	0	$0
4A-CI-00-16-039	FISMA FY 2016	11/09/2016	26	4	0	$0
4A-CI-00-17-014	OPM's Security Assessment and Authorization	06/20/2017	4	3	0	$0
1C-GA-00-17-010	ISG&AC @ MVP Health Care	06/30/2017	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	10/27/2017	39	8	0	$0
4A-CI-00-18-022	OPM's FY 2017 IT Modernization Expenditure	02/15/2018	4	1	0	$0
4A-HR-00-18-013	OPM's USA Staffing System	05/10/2018	4	2	0	$0
4A-CI-00-18-038	FISMA FY 2018	10/30/2018	52	13	0	$0

Information Systems Audits						
			Total # of Recs	# of Open Procedural Findings	Monetary Findings	
Report Number	Name	Date			# Open	Amount
1C-8W-00-18-036	ISG&AC @ UPMC	03/01/2019	5	1	0	$0
1C-LE-00-18-034	ISG&AC @ Priority Health	03/05/2019	10	1	0	$0
4A-CI-00-18-037	FITARA	04/25/2019	5	4	0	$0
4A-CF-00-19-026	OPM's CBIS	10/03/2019	7	1	0	$0
4A-CI-00-19-008	OPM's Compliance with Data Center Optimization	10/23/2019	23	8	0	$0
4A-CI-00-19-029	FISMA FY 2019	10/29/2019	47	14	0	$0
4A-CI-00-20-007	OPM's eOPF	06/30/2020	3	1	0	$0
4A-CI-00-20-009	OPM's Security Assessment & Authorization	09/18/2020	11	8	0	$0
4A-CI-00-20-008	OPM's Agency Common Controls	10/30/2020	4	3	0	$0
4A-CI-00-20-010	FISMA FY 2020	10/30/2020	45	15	0	$0
1C-A8-00-20-019	ISG&AC @ Scott and White Health Plan	12/14/2020	12	2	0	$0
1C-GG-00-20-026	ISG&AC @ Geisinger Health Plan	03/09/2021	2	1	0	$0
1C-SF-00-21-005	ISG&AC @ Selecthealth	09/13/2021	12	2	0	$0
4A-ES-00-21-020	OPM’s ESCS	09/30/2021	14	1	0	$0
4A-CI-00-21-012	FISMA FY 2021	10/27/2021	36	19	0	$0
1D-80-00-21-025	ISG&AC @ EmblemHealth	03/21/2022	5	2	0	$0
2022-ISAG-006	ISG&AC @ BCBS Alabama	8/22/2022	2	1	0	$0
35	Total Reports		615	138	0	$0

Experience-Rated Health Insurance Audits						
			Total # of Recs.	# of Open Procedural Recs.	Monetary Findings	
Report Number	Name	Date			# Open	Amount
1A-10-17-21-018	Audit of Health Care Service Corporation	2/23/22 3/16/22	18	4	0	$0
1B-45-00-21-034	Audit of Mail Handlers Benefit Plan	8/16/22	4	2	1	$204,073
1A-10-15-21-023	Audit of BCBS of Tennessee	08/25/22	11	1	1	$607,204
3	**Total Reports**		33	7	2	$811,277

Community-Rated Health Insurance Audits						
			Total # of Recs.	# of Open Procedural Recs.	Monetary Findings	
Report Number	Name	Date			# Open	Amount
1C-8W-00-20-017	UPMC Health Plan, Inc.	6/21/2021	17	4	2	$13,786,995
1C-QA-00-21-003	Independent Health Association, Inc.	1/7/2022	33	2	0	$0
1C-59-00-20-043	Kaiser Foundation Health Plan	08/16/2022	16	1	0	$0
3	**Total Reports**		66	5	2	$13,786,995

Other Insurance Audits						
			Total # of Recs.	# of Open Procedural Recs.	Monetary Findings	
Report Number	Name	Date			# Open	Amount
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
1H-07-00-19-017	CareFirst BlueChoice's Pharmacy Operations as Administered by CVS Caremark	7/20/2020	8	2	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	7	0	$0
1H-99-00-20-016	Audit of the Reasonableness of Selected FEHBP Carrier' Pharmacy Benefit Contracts	7/29/21	3	3	0	$0
1G-LT-00-21-013	Audit of the Federal Long Term Care Insurance Program	9/12/2022	3	2	0	$0
5	**Total Reports**		40	16	1	$834,425

Evaluations						
Report Number	**Name**	**Date**	**Total # of Recs.**	**# of Open Procedural Recs.**	**Monetary Findings**	
					# Open	**Amount**
004K-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
3	**Total Reports**		13	9	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
2022-SAG-007	Audit of the 2018 and 2019 Combined Federal Campaigns	9/7/2022	2	0	1	$164,212
L-2018-1	Review of OPM's Non-Public Decision to Re-Apportion Annuity Supplements	2/5/2018	3	3	0	$0
4A-DO-00-20-041	Delegation of Authority to Operate and Maintain the Theodore Roosevelt Federal Building and the Federal Executive Institute	8/5/2020	4	2	0	$0
4A-HI-00-18-026	FEHBP Program Integrity Risks Due to Contractual Vulnerabilities	4/1/2021	11	11	0	$0
N/A	PMF Application Process Redesign	05/18/2022	8	8	0	$0
6	**Total Reports**		31	26	1	$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: https://oig.opm.gov/contact/hotline

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