



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

Open Recommendations

**Open Recommendations Over Six Months Old as of
September 30, 2017**

December 1, 2017

EXECUTIVE SUMMARY

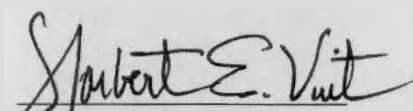
Open Recommendations Over Six Months Old as of September 30, 2017

December 1, 2017

Why Did We Prepare This Report?

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

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



Norbert E. Vint
Acting Inspector General

What Did We Find?

As of September 30, 2017, there were 214 outstanding recommendations contained in reports that the OIG had issued to the U.S. Office of Personnel Management over six months ago.

Type of Report	# of Reports	Total # Recs. Made	# Open Recs. as of 9/30/17
Internal Operations Audits	19	110	66
Info. Systems Audits	17	305	107
Experience-Rated Insurance Audits	6	43	20
Community-Rated Insurance Audits	3	10	6
Other Benefit Audits	2	15	9
Combined Federal Campaign Audits	1	2	2
Evaluations	2	8	4
Total	50	493	214

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 Operations Audits	65	1	\$108,880,417
Info. Systems Audits	107	0	\$0
Experience-Rated Insurance Audits	9	11	\$69,382,654
Community-Rated Insurance Audits	1	5	\$13,042,716
Other Benefit Audits	2	7	\$2,254,117
Combined Federal Campaign Audits	0	3	\$170,266
Evaluations	4	0	\$0
Total	188	26	\$193,730,170

ABBREVIATIONS

AFR	Annual Financial Report
AUP	Agreed-Upon Procedures
BCBS	BlueCross BlueShield
CFC	Combined Federal Campaign
COB	Coordination of Benefits
GSA	General Services Administration
FAR	Federal Acquisition Regulation
FEDVIP	Federal Employees Dental/Vision Insurance Program
FEGLI	Federal Employees Group Life 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
HRS	Human Resources Solutions
IHS	Indian Health Service
IPA	Independent Public Accountant
IPERA	Improper Payments Elimination and Recovery Act
LFCC	Local Federal Coordinating Committee
LII	Lost Investment Income
MLR	Medical Loss Ratio
N/A	Not Applicable
OBRA 90	Global Omnibus Budget Reconciliation Act of 1990
OCFC	Office of the Combined Federal Campaign
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

	<u>Page</u>
ABBREVIATIONS.....	i
I. INTERNAL OPERATIONS AUDITS.....	1
II. INFORMATION SYSTEM AUDITS.....	32
III. EXPERIENCE-RATED INSURANCE AUDITS.....	67
IV. COMMUNITY-RATED INSURANCE AUDITS.....	76
V. OTHER BENEFIT AUDITS.....	79
VI. COMBINED FEDERAL CAMPAIGN AUDITS.....	83
VII. EVALUATIONS.....	84
APPENDIX A: OVERVIEW CHARTS.....	86

I. INTERNAL OPERATIONS AUDITS

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

Title: Audit of the Fiscal Year 2008 Financial Statements		
Report #: 4A-CF-00-08-025		
Date: November 14, 2008		
Rec. #		
1	<i>Finding</i>	<u>Information Systems General Control Environment</u> –Security policies and procedures have not been updated to incorporate current authoritative guidance and the procedures performed to certify and accredit certain financial systems were not complete. In addition, it was noted that application access permissions have not been fully documented to describe the functional duties the access provides to assist management in reviewing the appropriateness of system access. Also, there were instances where background investigations and security awareness training was not completed prior to access being granted.
	<i>Recommendation</i>	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.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

Title: Audit of the Fiscal Year 2009 Financial Statements
Report #: 4A-CF-00-09-037
Date: November 13, 2009

Rec. #		
1	Finding	<u>Information Systems General Control Environment</u> – Information system general control deficiencies identified in previous years related to OPM and its programs continue to persist or have not been fully addressed and consequently are not in full compliance with authoritative guidance.
	Recommendation	KPMG recommends that the Office of the Chief Information Officer should continue to update and implement entity-wide policies and procedures and provide more direction and oversight to Program Offices for completing and appropriately overseeing certification and accreditation requirements and activities. In addition, documentation on application access permissions should be enhanced and linked with functional duties and procedures for granting logical and physical access needs to be refined to ensure access is granted only to authorized individuals. Finally, policies and procedures should be developed and implemented to ensure POA&Ms are accurate & complete.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

Title: Audit of the Fiscal Year 2010 Financial Statements
Report #: 4A-CF-00-10-015
Date: November 10, 2010

Rec. #		
1	Finding	<u>Information Systems General Control Environment</u> – Deficiencies in OPM's and the Programs' information system general controls that were identified and reported as a significant deficiency in previous years continue to persist. Although changes in information system management during this fiscal year, including the appointment of a new Chief Information Officer (CIO) and Senior Agency Information Security Officer, have resulted in plans to address these weaknesses, these plans have not yet been fully executed to resolve long-standing deficiencies in OPM's security program.
	Recommendation	KPMG recommends that the CIO develop and promulgate entity-wide security policies and procedures and assume more responsibility for the coordination and oversight of Program Offices in completing certification and accreditation and other information security requirements and activities.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

Continued: Audit of the Fiscal Year 2010 Financial Statements

Rec. #		
2	Finding	<u>Information Systems General Control Environment</u> – See number 1 above
	Recommendation	KPMG recommends that the CIO identify common controls, control responsibilities, boundaries and interconnections for information systems in its system inventory.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
3	Finding	<u>Information Systems General Control Environment</u> – See number 1 above
	Recommendation	KPMG recommends that the CIO implement a process to ensure the POA&Ms remains accurate and complete.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

Title: Stopping Improper Payments to Deceased Annuitants

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

Date: September 14, 2011

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

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

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

Rec. #		
1	Finding	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to address the information system control environment weaknesses.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

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

Rec. #		
1	Finding	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to address the information system control environment weaknesses.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

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

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

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

Rec. #		
1	Finding	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to address the information system control environment weaknesses.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

Title: Audit of OPM's Fiscal Year 2013 Improper Payments Reporting
Report #: 4A-CF-00-14-009
Date: April 10, 2014

Rec. #		
1	Finding	<u>Weak Oversight Controls over Improper Payment Reporting</u> - We identified several inaccuracies between what was reported in the AFR and the supporting documentation that we obtained from the program offices.
	Recommendation	The OIG recommends that OPM strengthen its oversight controls over the improper payments data reported in the Agency Financial Report to ensure that it accurately reflects supporting data.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the reporting of improper payments data, it will increase OPM's effectiveness in ensuring that IPERA requirements are met and the accuracy of information reported in the Agency Financial Report.

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

Rec. #		
1	Finding	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.
	Recommendation	KPMG recommends that the OPM Director in coordination with the CIO and system owners, including the Chief Financial Officer and system owners in Program offices, ensure that resources are prioritized and assigned to implement the current authoritative guidance regarding two-factor authentication.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

<i>Continued: Audit of OPM's Fiscal Year 2014 Financial Statements</i>		
Rec. #		
2	<i>Finding</i>	<u>Information Systems Control Environment</u> - Access rights in OPM systems are not documented and mapped to personnel roles and functions to ensure that personnel access is limited only to the functions needed to perform their job responsibilities.
	<i>Recommendation</i>	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."
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
3	<i>Finding</i>	<u>Information Systems Control Environment</u> - The information security control monitoring program was not fully effective in detecting information security control weaknesses. We noted access rights in OPM systems were: <ul style="list-style-type: none"> • 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.
	<i>Recommendation</i>	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: <ul style="list-style-type: none"> • 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.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

Title: Audit of OPM's Compliance with the Freedom of Information Act
Report #: 4K-RS-00-14-076
Date: March 23, 2015

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

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

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

Date: April 13, 2015

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

Title: Audit of OPM's Fiscal Year 2014 Improper Payments Reporting

Report #: 4A-CF-00-15-025

Date: May 15, 2015

Rec. #		
1	Finding	<u>Improper Payments Information in the AFR was Inaccurately Reported</u> - During our audit we identified several inaccuracies between what was reported in the FY 2014 AFR and the supporting documentation that we obtained from the program offices.
	Recommendation	The OIG recommends that OPM strengthen its oversight controls over the improper payments data reported in the Agency Financial Report to ensure that it accurately reflects supporting data. (Rolled-Forward from FY 2013)
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the reporting of improper payments data, it will increase OPM's effectiveness in ensuring that IPERA requirements are met and the accuracy of information reported in the Agency Financial Report.

Continued: Audit of OPM's Fiscal Year 2014 Improper Payments Reporting

Rec. #		
4	Finding	<u>Improper Payments Information in the AFR was Insufficient or Unsupported</u> - We found that OPM could not provide or had insufficient documentation to support improper payments information reported in the AFR.
	Recommendation	The OIG recommends that OCFO strengthen their procedures to ensure that the improper payments information reported in OPM's AFR is supported, reviewed, and validated for accuracy prior to the information's inclusion in the AFR.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the reporting of improper payments data, it will increase OPM's effectiveness in ensuring that IPERA requirements are met and the accuracy of information reported in the Agency Financial Report.

Title: Audit of Human Resources Solutions' Pricing Methodologies

Report #: 4A-HR-00-13-055

Date: June 2, 2015

Rec. #		
1	Finding	<u>Pricing Methodologies Were Not Fully Supported</u> - While assessing the reasonableness of the costing tools that were used to develop FY 2014 prices, the OIG determined that pricing methodologies, including cost inputs, were not fully supported.
	Recommendation	The OIG recommends that HRS develop policies and procedures for creating the monthly Financial Snapshot Report by RMG. The policies and procedures should include a discussion of documentation retention, underlying assumptions, and the methodology used to develop and allocate the cost pools.
	Status	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and corrective actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Documented guidance regarding the process for creating RMG's Financial Snapshot Report and documented process to allocate their Cost Pool 4 amounts will decrease the likelihood of under- or over-charging customer agencies.

<i>Continued: Audit of Human Resources Solutions' Pricing Methodologies</i>		
Rec. #		
2	<i>Finding</i>	<u>Pricing Methodologies Were Not Fully Supported</u> - While assessing the reasonableness of the costing tools that were used to develop FY 2014 prices, the OIG determined that pricing methodologies, including cost inputs, were not fully supported.
	<i>Recommendation</i>	The OIG recommends that HRS develop policies and procedures for the determinations of fees charged by its program areas to customer agencies. The policies and procedures should include a discussion of document retention, underlying assumptions, and the methodology used to determine its rates.
	<i>Status</i>	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and corrective actions are in progress. Evidence to support closure has not yet been provided.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Documented guidance regarding the support for pricing determinations will decrease the likelihood of under- or over-charging customer agencies.
3	<i>Finding</i>	<u>Pricing Methodologies Were Not Fully Supported</u> - While assessing the reasonableness of the costing tools that were used to develop FY 2014 prices, we determined that pricing methodologies, including cost inputs, were not fully supported.
	<i>Recommendation</i>	The OIG recommends that HRS strengthen their internal controls to ensure that the inputs used in HRS's pricing calculations are properly reviewed, approved, and documented.
	<i>Status</i>	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and corrective actions are in progress. Evidence to support closure has not yet been provided.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Documented guidance regarding the support for pricing determinations will decrease the likelihood of under- or over-charging customer agencies.

<i>Continued: Audit of Human Resources Solutions' Pricing Methodologies</i>		
Rec. #		
4	<i>Finding</i>	<u>Prices for FY 2013 and 2014 Services Were Not Fully Supported</u> – The OIG found that Administrative Law Judges (ALJ) did not have sufficient documentation to support prices charged to customers in FY 2013. Specifically, ALJ provided documents to support Cost Pools 1 and 2 for FY 2013; however, we were unable to determine how the documents supported 24 out of 25 of the expense categories used in Cost Pools 1 and 2. In addition, we found that a majority of HRS program areas did not have sufficient documentation to support prices charged to customers in FY 2014.
	<i>Recommendation</i>	The OIG recommends that HRS develop policies and procedures that include a discussion of documentation retention for the methodology and applicable supporting documents used to determine its prices charged to customer agencies.
	<i>Status</i>	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and corrective actions are in progress. Evidence to support closure has not yet been provided.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	If controls are in place to ensure documentation retention for the methodology and applicable supporting documents used to determine HRS prices to customer agencies, then the risk of customer agencies being under- or over-charged will decrease.
5	<i>Finding</i>	<u>Prices for FY 2013 and 2014 Services Were Not Fully Supported</u> - One out of six Training and Management Assistance Program (TMAP) projects sampled did not have documentation to support the project costs (i.e., costing tools and interagency agreements). TMAP stated that they created this project in error. TMAP provided a Consolidated Business Information System screenshot that stated the project is "in progress"; however, there was no confirmation that the project was cancelled.
	<i>Recommendation</i>	The OIG recommends that HRS strengthen their internal controls to ensure that projects are properly reviewed and approved to prevent projects created in error.
	<i>Status</i>	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and corrective actions are in progress. Evidence to support closure has not yet been provided.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	If controls are in place to ensure proper review and approval of HRS projects, then the risk of customer agencies being under- or over-charged will decrease.

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

Rec. #		
1	<i>Finding</i>	<u>Information Systems Control Environment</u> - The current authoritative guidance regarding two-factor authentication has not been fully applied.
	<i>Recommendation</i>	KPMG recommends that the OCIO fully implement the current authoritative guidance regarding two-factor authentication.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
2	<i>Finding</i>	<u>Information Systems Control Environment</u> - Access rights in OPM systems are not documented and mapped to personnel roles and functions to ensure that personnel access is limited only to the functions needed to perform their job responsibilities.
	<i>Recommendation</i>	KPMG recommends that the OCIO document and map access rights in OPM systems to personnel roles and functions, following the principle of "least privilege".
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

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

Rec. #		
3	Finding	<p><u>Information Systems Control Environment</u> - The information security control monitoring program was not fully effective in detecting information security control weaknesses. We noted access rights in OPM systems were:</p> <ul style="list-style-type: none"> • Granted to new users without following the OPM access approval process and quarterly reviews to confirm access approval were not consistently performed. • Not revoked immediately upon user separation and quarterly reviews to confirm access removal were not consistently performed. • Granted to a privileged account without following the OPM access approval process.
	Recommendation	<p>KPMG recommends that the OCIO enhance OPM's information security control monitoring program to detect information security control weaknesses by:</p> <ul style="list-style-type: none"> • Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process; and • Monitoring the process for the identification and removal of separated users to ensure that user access is removed timely upon separation; implementing procedures to ensure that user access, including user accounts and associated roles, are reviewed on a periodic basis consistent with the nature and risk of the system, and modifying any necessary accounts identified.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
4	Finding	A formalized system component inventory of devices to be assessed as part of vulnerability or configuration management processes was not maintained.
	Recommendation	KPMG recommends that the OCIO continue to perform, monitor, and improve its patch and vulnerability management processes, to include maintaining an accurate inventory of devices.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.

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

Rec. #		
5	<i>Finding</i>	Entity Level Controls Over Financial Management - During FY 2015 OPM reported a data breach which affected millions of Federal employees and government contractors. Based on KPMG's procedures to evaluate the potential impact of the data breach on OPM's financial statements, KPMG noted a number of control deficiencies that are pervasive throughout the agency.
	<i>Recommendation</i>	KPMG recommends that the OCFO perform a thorough review of OPM's entity-level controls over financial reporting and relevant activities to identify the underlying cause of these deficiencies and take the appropriate corrective actions to strengthen controls to mitigate risk of material misstatement when non-routine events occur.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Continued improvement in entity-level controls over financial management may improve the effectiveness of OPM's response to non-routine events and transactions and enhance the likelihood of the timely detection and correction of material misstatements in the financial statements.

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

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

Continued: Special Review of OPM's Award of a Credit Monitoring and Identity Theft Services Contract to Winvale Group LLC, and its Subcontractor, CSIdentity

Rec. #		
2	Finding	See number 1 above for description.
	Recommendation	The OIG recommends that OPO implement controls to ensure that each contract is in compliance with the FAR requirements and contracting actions are documented and approved prior to contract award.
	Status	The agency agreed with the recommendation. OPM has informed us that a corrective action plan has been developed and corrective actions are in progress. Evidence to support closure has not yet been provided.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If effective controls are in place to ensure the contract is in compliance, it will increase the likelihood that OPM is obtaining a qualified vendor.

Title: Audit of OPM's Fiscal Year 2015 Improper Payments Reporting

Report #: 4A-CF-00-16-026

Date: May 11, 2016

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

Continued: Audit of OPM's Fiscal Year 2015 Improper Payments Reporting

Rec. #		
3	Finding	<u>Risk Assessments</u> - When reviewing the risk assessment results, the OIG found assessments with no or insufficient documentation to support the results reported in OPM's FY 2015 Agency Financial Report.
	Recommendation	The OIG recommends that the OCFO re-evaluate the risk assessments performed over the Background Investigations, Federal Employees' Group Life Insurance, Vendor Payments, Travel Card, and Payroll programs to ensure that programs are not susceptible to significant improper payments.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the reporting of improper payments data, it will increase OPM's effectiveness in ensuring that IPERA requirements are met and the accuracy of information reported in the Agency Financial Report.
4	Finding	<u>Risk Assessments</u> - See number 3 above.
	Recommendation	The OIG recommends that the OCFO strengthen their procedures to ensure that the improper payments information reported in OPM's Agency Financial Report is supported, reviewed, and validated for accuracy prior to the information's inclusion in the Agency Financial Report. (Rolled-Forward from FY 2014)
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the reporting of improper payments data, it will increase OPM's effectiveness in ensuring that IPERA requirements are met and the accuracy of information reported in the Agency Financial Report.
5	Finding	<u>Improper Payments Information in the Agency Financial Report Was Inaccurately Reported</u> - During the audit the OIG identified inaccuracies between what was reported in the FY 2015 Agency Financial Report and the supporting documentation that we obtained from the OCFO.
	Recommendation	The OIG recommends that the OCFO strengthen its oversight controls over the improper payments data reported in the Agency Financial Report to ensure that it accurately reflects supporting data. (Rolled-Forward from FY 2013 and FY 2014)
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the reporting of improper payments data, it will increase OPM's effectiveness in ensuring that IPERA requirements are met and the accuracy of information reported in the Agency Financial Report.

<i>Continued: Audit of OPM's Fiscal Year 2015 Improper Payments Reporting</i>		
Rec. #		
6	<i>Finding</i>	<u>Improper Payments Information in the Agency Financial Report Was Inaccurately Reported</u> - See number 5 above
	<i>Recommendation</i>	The OIG recommends that in the FY 2016 Agency Financial Report, OCFO correct all of the errors identified in the FY 2015 Agency Financial Report Table 14, Status of Internal Controls.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	If controls are in place over the reporting of improper payments data, it will increase OPM's effectiveness in ensuring that IPERA requirements are met and the accuracy of information reported in the Agency Financial Report

Title: Audit of OPM's Office of Procurement Operations' Contract Management Process		
Report #: 4A-CA-00-15-041		
Date: July 8, 2016		
Rec. #		
1	<i>Finding</i>	<u>OPO Lacks Strong Internal Controls Over Its Contract Management Operations</u> - On April 23, 2015, Calyptus issued their Strategic Assessment Report to OPO, which identified 16 recommendations for OPO. We reviewed Calyptus' Strategic Assessment Report of OPO and supporting documentation, and determined that the findings and recommendations reported by Calyptus are valid and logical. However, OPM is not ensuring that OPO takes appropriate corrective action to address the internal control deficiencies identified.
	<i>Recommendation</i>	The OIG recommends that OPO strengthen its internal controls by working with OPM's Internal Oversight and Compliance office to implement corrective actions to address the findings and recommendations reported in the Strategic Assessment Report issued by Calyptus Consulting Group, Inc., on April 23, 2015.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are free from deficiencies.

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

Rec. #		
2	Finding	<u>Inaccurate Contract Amounts Reported in OPM's Information Systems</u> - We requested access to 60 contract files with open obligations reported in the OCFO's CBIS Fiscal Years 2010 to 2014 Open Obligation Report, and determined that the contract amounts reported in the CBIS for 22 of the 60 contracts sampled differed from the contract amounts reported in OPO's contract files. In addition, OPO was unable to provide 17 of the 60 contract files, so we cannot determine if the amounts reported in CBIS were accurate.
	Recommendation	The OIG recommends that OPO implement internal controls to ensure that contract data, including contract award amounts, is accurately recorded in OPM's information systems, such as CBIS, and the appropriate supporting documentation is maintained.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are appropriately reported in OPM's financial management system.
3	Finding	<u>Weak Controls over the Contract Closeout Process</u> - OPO could not provide a listing of contract closeouts for FY 2013 and FY 2014. In addition, of the 60 contracts the OIG sampled, we identified 46 in which OPO did not initiate the contract closeout process in compliance with the FAR.
	Recommendation	The OIG recommends that OPO develop an accurate inventory of FYs 2013 and 2014 contracts ready for closeout.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.
4	Finding	<u>Weak Controls over the Contract Closeout Process</u> - See number 3 above.
	Recommendation	The OIG recommends that OPO establish and implement management controls to ensure that contracts are tracked and managed through the closeout process and adequate documentation is maintained in the contract file, including evidence of contract completion and closeout.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.

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

Rec. #		
5	Finding	<u>Weak Controls over the Contract Closeout Process</u> - See number 3 above.
	Recommendation	The OIG recommends that OPO provide documentation to verify that the closeout process has been administered on the open obligations for the 46 contracts questioned.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.
6	Finding	<u>Weak Controls over the Contract Closeout Process</u> - As a result of the control deficiencies identified for the contract closeout process, as well as the issues previously discussed, we cannot determine if \$108,880,417 in remaining open obligations, associated with 46 questioned contracts, are still available for use by OPM's program offices.
	Recommendation	The OIG recommends that OPM's Office of Procurement Operations return \$108,880,417 in open obligations, for the 48 contracts questioned, to the program offices if support cannot be provided to show that the contract should remain open and the funds are still being utilized.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	\$108,880,417
	Other Nonmonetary Benefit	If controls are in place over the contract management process, it will increase OPM's effectiveness in ensuring that acquisition requirements are met and contracts are properly closed out.

Title: Audit of OPM's Fiscal Year 2016 Financial Statements

Report #: 4A-CF-00-16-030

Date: November 14, 2016

Rec. #		
1	Finding	<u>Information Systems Control Environment</u> The Information Security and Privacy Policy Handbook is outdated.
	Recommendation	Grant Thornton recommends that OPM review, update and approve the OPM ISPP Handbook at the organization defined frequency. The review should include the following: <ul style="list-style-type: none"> • Updating language to reflect procedures actually in place (e.g., updating the frequency of the review / updates of POA&Ms). • Removing outdated procedures and terminology (e.g., removing the use of the term "Designated Security Officer" throughout).
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.

	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Policies will reflect current operational environment, which will allow personnel to develop and adhere to authorized processes and related controls.

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

Rec. #		
2	Finding	<u>Information Systems Control Environment</u> OPM System Documentation is outdated.
	Recommendation	Grant Thornton recommends that OPM create and/or update system documentation corresponding to the in-scope systems and applications. Specifically, <ul style="list-style-type: none"> • SSPs – We recommend OPM update and finalize the SSPs for the in-scope applications and systems, and review the SSPs according to organization defined frequencies. • RAs – We recommend OPM conduct a RA for the in-scope applications and systems and document comprehensive results of the testing performed. • ATO – We recommend OPM perform SA&A reviews in a timely manner and create up-to-date ATO packages for the in-scope applications and systems. • ISCM – We recommend OPM document results of ISCM testing performed for all in-scope applications and systems.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Complete and consistent security control documentation and complete and thorough testing will allow the agency to be informed of security control weaknesses that threaten the confidentiality, integrity, and availability of the data contained within its systems.
3	Finding	<u>Information Systems Control Environment</u> - The FISMA Inventory Listing is incomplete.
	Recommendation	Grant Thornton recommends that OPM document the interfaces that interact with each system / application within the FISMA Inventory Listing and also perform a thorough review of the FISMA Inventory System listing on a periodic basis to determine whether the information documented is complete and accurate. Management should document their review of the FISMA Inventory Listing for record retention purposes.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	With an updated FISMA Inventory Listing, Management can: (a) work towards FISMA compliance, (b) develop an understanding of how transactions/data flow between the various systems, and (c) understand the totality of operational systems/applications within its environment.

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

Rec. #		
4	Finding	<u>Information Systems Control Environment</u> OPM lacks a system generated listing of terminated agency contractors.
	Recommendation	Grant Thornton recommends that OPM implement a system/control that tracks terminated contractors, much like the HR system does for government employees.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	A listing of terminated contractors to be reconciled against systems access will decrease the risk that users retain lingering access to systems and therefore will decrease the risk of inaccurate, invalid, and unauthorized transactions being processed by systems that could ultimately impact financial reporting.
5	Finding	<u>Information Systems Control Environment:</u> Role based training has not been completed.
	Recommendation	Grant Thornton recommends that OPM establish an automated means of documenting a list of users with SISR responsibilities. If OPM is unable to establish an automated means of documenting this listing, Management should establish a control whereby a user or group of users is tasked with reviewing the manually assembled listing on a periodic basis to make sure the listing is complete and accurate.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Individuals obtain skills / training needed to perform day to day duties.
6	Finding	<u>Information Systems Control Environment:</u> The Information System Security Officer positions are vacant.
	Recommendation	Grant Thornton recommends that OPM fill the vacant IT positions or designate existing personnel to perform the responsibilities of these vacant positions.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	N/A

<i>Continued: Audit of OPM's Fiscal Year 2016 Financial Statements</i>		
Rec. #		
7	<i>Finding</i>	<u>Information Systems Control Environment</u> : Lack of Monitoring of Plan of Actions and Milestones (POA&Ms)
	<i>Recommendation</i>	Grant Thornton recommends that OPM assign specific individuals with overseeing/monitoring POA&Ms to ensure they are addressed in a timely manner.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	The agency is able to determine whether vulnerabilities are remediated in a timely manner. This decreases the risk that systems are compromised.
8	<i>Finding</i>	<u>Information Systems Control Environment</u> : Lack of periodic access recertifications.
	<i>Recommendation</i>	Grant Thornton recommends that OPM perform a comprehensive review of personnel with access to the in-scope applications/systems at the organization defined frequencies. The review should include the following: <ul style="list-style-type: none"> • Personnel retain appropriate access to the in-scope applications / systems. • Terminated personnel do not currently retain access to the in-scope applications / systems.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	A comprehensive review of personnel with access to the in-scope applications /systems will decrease the risk that inappropriate individuals maintain access allowing them to perform incompatible functions or functions associated with elevated privileges.
9	<i>Finding</i>	<u>Information Systems Control Environment</u> : The active directory password settings are non-compliant.
	<i>Recommendation</i>	Grant Thornton recommends that all system owners perform a detailed review to ensure that password configuration settings align with organization policies/ procedures and industry best practices.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Updated password settings will disallow users from reusing passwords more frequently, and will disable accounts after 120 days of inactivity to prevent potentially terminated users (or users that do not require access) from retaining access and performing unauthorized transactions.

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

Rec. #		
10	<i>Finding</i>	<u>Information Systems Control Environment</u> : The physical access to the data center is not appropriately restricted.
	<i>Recommendation</i>	Grant Thornton recommends that OPM: <ul style="list-style-type: none"> • Permanently lock the door between certain rooms so that users cannot gain access to the rooms via the door, or • Implement a card reader for the door so that users can only access certain rooms if they have approved physical access.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	N/A
11	<i>Finding</i>	<u>Information Systems Control Environment</u> : The FACES audit logs are not periodically reviewed.
	<i>Recommendation</i>	Grant Thornton recommends that system owners or delegates review the FACES Invalid Login audit records periodically to monitor for violations or suspicious activity. If violations or suspicious activity occurs, we recommend that the system owners or delegates follow up with the responsible individual and/or elevate the issues to the Security Operations Team for review. The review of audit logs should be documented for record retention purposes. Additionally, the management should also specify the frequency of the review.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	A thorough review of audit logs decreases the risk that suspicious activity that occurs may go undetected and therefore may not be addressed in a timely manner.
12	<i>Finding</i>	<u>Information Systems Control Environment</u> : Journal voucher preparers and approvers cannot be identified.
	<i>Recommendation</i>	Grant Thornton recommends that OPM devise a way (e.g., create a custom query) to create a system-generated listing of users that can input and approve journal vouchers.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	N/A

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

Rec. #		
13	Finding	<u>Information Systems Control Environment</u> : Lack of access descriptions and Segregation of Duties (SoD) Matrices.
	Recommendation	Grant Thornton recommends that OPM perform a thorough review of the use access rights, and document the following: <ul style="list-style-type: none"> • Description of each role / group that has system access in plain English. • Privileges that are associated to each role/group in plain English. For instance the "Journal Entry" group has access to create and input information into a journal entry. • Description of actions/activities that each privilege can perform in plain English. • Population of conflicting duties (i.e., individual cannot sign and approve a journal voucher)
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	A comprehensive understanding of user access rights will decrease the risk that users perform incompatible duties or have access to privileges or roles outside of what is needed to perform their day-to-day duties.
14	Finding	<u>Information Systems Control Environment</u> : [REDACTED] are not PIV-compliant.
	Recommendation	Grant Thornton recommends that OPM create and implement a plan to enforce two-factor authentication for each of its applications, including the financially relevant applications mentioned above.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Two factor authentication will decrease the risk of unauthorized access into OPM systems.
15	Finding	<u>Information Systems Control Environment</u> : Access procedures for terminated users are not followed.
	Recommendation	Grant Thornton recommends that OPM ensures proper termination processes (e.g., return of PIV badges and IT equipment, completion of Exit Clearance Forms and completion of exit surveys) are followed in a timely manner, and additionally, that documentation of completion of these processes is maintained.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Ensuring proper termination procedures are followed will decrease the risk that individuals gain / retain unauthorized access to IT resources/systems.

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

Rec. #		
16	Finding	<u>Information Systems Control Environment</u> : OPM lacks configuration management policies governing changes to the mainframe environment.
	Recommendation	Grant Thornton recommends that OPM establish a comprehensive configuration management plan that includes roles, responsibilities, and outlines details supporting authorization, testing and documentation requirements. These policies and procedures should be made available to personnel responsible for making changes to the mainframe.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Decreases the risk that unauthorized or erroneous changes to the mainframe configuration may be introduced without detection by system owners.
17	Finding	<u>Information Systems Control Environment</u> : OPM is unable to generate a complete and accurate listing of modifications to the mainframe and midrange.
	Recommendation	Grant Thornton recommends that OPM system owners establish a methodology to systematically track all configuration items that are migrated to production, and be able to produce a complete and accurate listing of all configuration items for both internal and external audit purposes, which will in turn support closer monitoring and management of the configuration management process.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Decreases the risk that unauthorized or erroneous changes to the mainframe and midrange configuration may be introduced without detection by system owners
18	Finding	<u>Information Systems Control Environment</u> : OPM lacks a security configuration checklist
	Recommendation	Grant Thornton recommends that OPM enforce existing policy requiring mandatory security configuration settings, developed by OPM or developed by vendors or federal agencies, are implemented and settings are validated on a periodic basis to ensure appropriateness.
	Status	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Restrictive security settings in place for components and a periodic assessment to ensure that such settings are in place and appropriate decreases the risk that the confidentiality, integrity, and / or availability of financial data is compromised.

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

Rec. #		
19	<i>Finding</i>	<u>Information Systems Control Environment</u> : An accurate listing of modifications to ██████████ cannot be generated.
	<i>Recommendation</i>	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.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Decreases the risk that unauthorized or erroneous changes to the applications' configuration may be introduced without detection by system owners
20	<i>Finding</i>	<u>Information Systems Control Environment</u> : A complete and accurate listing of modifications to FACES cannot be generated.
	<i>Recommendation</i>	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.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Decreases the risk that unauthorized or erroneous changes to the application's configuration may be introduced without detection by system owners
21	<i>Finding</i>	<u>Information Systems Control Environment</u> : The access to the FACES production environment is not appropriately restricted
	<i>Recommendation</i>	Grant Thornton recommends that OPM should segregate duties between user roles with development responsibilities and user roles with access to the production environment. Further, OPM should implement and operate monitoring controls to verify only authorized and valid changes are implemented into restricted.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	N/A

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

Rec. #		
22	<i>Finding</i>	<u>Monitoring Internal Controls: A-123 Management's Responsibility for Internal Control</u>
	<i>Recommendation</i>	Grant Thornton recommends that OPM strengthen the annual internal assessments, testing and documentation based on OMB A-123, Appendix A guidance.
	<i>Status</i>	The agency agreed with the recommendation. OPM is taking corrective actions. As of September 30, 2017, the independent public accountant employed by OPM to conduct the financial statement audit had not received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	N/A

II. INFORMATION SYSTEM AUDITS

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

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

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

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

Title: Federal Information Security Management Act Audit Fiscal Year 2010		
Report #: 4A-CI-00-10-019		
Date: November 10, 2010		
Rec. #		
10	Finding	<u>Test of Security Controls</u> - FISMA requires agencies to test the security controls of their systems on an annual basis. In FY 2010, 15 systems did not have adequate security control tests.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
30	Finding	<u>Contingency Plan Testing</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2010, 13 systems were not subject to adequate contingency plan tests.
	Recommendation	The OIG recommends that OPM’s program offices test the contingency plans for each system on an annual basis. The contingency plans should be immediately tested for the 13 systems that were not subject to adequate testing in FY 2010.
	Status	OPM agreed with the recommendation. It is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

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

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

Title: Audit of the IT Security Controls of OPM's ARRTS
Report #: 4A-OP-00-12-013
Date: July 16, 2012

Rec. #		
1	Finding	<u>Independent Security Control Testing</u> - A security assessment was completed for ARRTS in December 2009 as a part of the system's certification and accreditation process. However, our review determined that the scope of this assessment was not accurately defined and therefore the security controls of ARRTS have not been adequately tested, as required by FISMA.
	Recommendation	The OIG recommends that an independent test of the system's security controls be conducted for ARRTS that fully tests all controls applicable to a FIPS 199 "low" system as mandated by NIST SP 800-53.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
7	Finding	<u>POA&M</u> - The ARRTS POA&M contained 10 security weaknesses, the majority of which have remediation activities in excess of 400 days overdue.
	Recommendation	The OIG recommends that the Owners of ARRTS develop a plan for the immediate remediation of all overdue POA&M items.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for tracking know information security weaknesses.
13	Finding	<u>System Auditing</u> - Once auditing is enabled, the Owners of ARRTS must ensure that the audit logs are routinely reviewed.
	Recommendation	The OIG recommends that the Owners of ARRTS routinely monitor/review audit logs generated by ARRTS.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for monitoring information system activity.
15	Finding	<u>Identifier Management</u> - There is no process in place to routinely audit active user accounts to look for duplicate accounts.
	Recommendation	The OIG recommends that the Owners of ARRTS implement a process to routinely audit all active user accounts to ensure that no unnecessary duplicate accounts exist.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for granting appropriate access to information systems.

Continued: Audit of the IT Security Controls of OPM's ARRTS

Rec. #		
17	Finding	<u>Personnel Termination</u> - There is no process in place to routinely audit active user accounts to look for active accounts assigned to terminated employees.
	Recommendation	The OIG recommends that the Owners of ARRTS periodically audit active ARRTS user accounts to verify that accounts do not remain open for individuals no longer employed at OPM and that the level of access granted remains appropriate.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for granting appropriate access to information systems.

Title: Federal Information Security Management Act Audit Fiscal Year 2012

Report #: 4A-CI-00-12-016

Date: November 9, 2011

Rec. #		
2	Finding	<u>Risk Management</u> - NIST SP 800-39 states that agencies should establish and implement "Governance structures [that] provide oversight for the risk management activities." The OCIO does not currently have a formal methodology for managing risk at an organization-wide level.
	Recommendation	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive Function.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security risks at OPM.
11	Finding	<u>Multi-factor Authentication</u> - OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by the beginning of FY 2012. However, as of the end of FY 2012, none of the 47 major systems at OPM require PIV authentication.
	Recommendation	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.

Continued: Federal Information Security Management Act Audit Fiscal Year 2012

Rec. #		
14	<i>Finding</i>	<u>Test of Security Controls</u> - FISMA requires agencies to test the security controls of its systems on an annual basis. In FY 2012, 13 systems were not subject to adequate security control tests.
	<i>Recommendation</i>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<i>Status</i>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
15	<i>Finding</i>	<u>Contingency Plan Testing</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2012, eight systems were not subject to adequate contingency plan tests.
	<i>Recommendation</i>	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.
	<i>Status</i>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for recovering from an unplanned system outage.

Title: Federal Information Security Management Act Audit Fiscal Year 2013

Report #: 4A-CI-00-13-021

Date: November 21, 2013

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

Continued: Federal Information Security Management Act Audit Fiscal Year 2013

Rec. #		
3	Finding	<u>Agency-wide Risk Management</u> - the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, as of the end of FY 2013, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were not all fully implemented.
	Recommendation	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security risks at OPM.
11	Finding	<u>Multi-factor Authentication</u> - OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by the beginning of FY 2012. However, as of the end of the FY 2013, none of the 47 major systems at OPM require PIV authentication.
	Recommendation	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.
13	Finding	<u>Test of Security Controls</u> - FISMA requires agencies to test the security controls of its systems on an annual basis. In FY 2013, 13 systems were not subject to adequate security control tests.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Management Act Audit Fiscal Year 2013

Rec. #		
14	Finding	<u>Contingency Plan Testing</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2013, seven were not subject to adequate contingency plan tests.
	Recommendation	The OIG recommends that OPM’s program offices test the contingency plans for each system on an annual basis. The contingency plans should be tested for the systems that were not subject to adequate testing in FY 2013 as soon as possible.
	Status	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

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

Rec. #		
1	Finding	<u>Security Assessment and Authorization (SA&A)</u> – DTP does not have a current SA&A package, nor an active authorization to operate.
	Recommendation	The OIG recommends that the DTP environment be subject to a complete and current SA&A process.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems are subject to a thorough security assessment.
2	Finding	<u>Continuous Monitoring of Security Controls</u> - OPM’s internal IT policies require that the IT security controls of each major application owned by a federal agency be tested on a continual basis. The owners of DTP did not submit continuous monitoring security reports in March or September, 2013, as required by OPM policy.
	Recommendation	The OIG recommends that DTP be subject to continuous monitoring of security controls in accordance with OPM policy.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

<i>Continued: Audit of IT Security Controls – OPM’s DTP</i>		
Rec. #		
4	<i>Finding</i>	<u>Configuration Change Control</u> - DTP application programmers have the technical ability to develop a change and move it into production without following the appropriate change control process.
	<i>Recommendation</i>	The OIG recommends that the OCIO make the appropriate system modifications to ensure appropriate segregation of duties are enforced within DTP.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for managing changes to information systems.
5	<i>Finding</i>	<u>Configuration Change Control</u> - DTP application programmers have the technical ability to develop a change and move it into production without following the appropriate change control process.
	<i>Recommendation</i>	The OIG recommends that the OCIO make the appropriate organizational modification to ensure a business unit independent of the application developers migrates changes into production. That same business unit should be responsible for validating that all elements of the SDLC were followed, changes were appropriately tested, and all documentation is valid and approved prior to migrating changes into production.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for managing changes to information systems.
6	<i>Finding</i>	<u>Duplicate Production Environments</u> - Currently, DTP is comprised of a development, test, and production environment. However, the production environment of DTP resides on the LAN/WAN and is not segregated from the production applications hosted on LAN/WAN. Essentially there are two production environments.
	<i>Recommendation</i>	The OIG recommends that the OCIO make the appropriate system modification to ensure that there is only one production environment in OPM's technical infrastructure.
	<i>Status</i>	This recommendation was closed after September 30, 2017.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for adequately segregating development, test, and production technical environments.

Title: Federal Information Security Management Act Audit Fiscal Year 2014
Report #: 4A-CI-00-04-031
Date: November 12, 2014

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

Continued: Federal Information Security Management Act Audit Fiscal Year 2014

Rec. #		
6	Finding	<u>Agency-wide Risk Management</u> - the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were not all fully implemented.
	Recommendation	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security risks at OPM.
7	Finding	<u>Baseline Configurations</u> - In FY 2014, OPM has continued its efforts toward formalizing baseline configurations for critical applications, servers, and workstations. At the end of the fiscal year, the OCIO had established baselines for several operating systems, but not for all that the agency uses in its environment.
	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, ██████, ██████, ██████, and ██████.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
Rec. #		
8	Finding	<u>Configuration Auditing</u> - There are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.
	Recommendation	The OIG recommends the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 7 has been completed.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that servers are in compliance with approved security settings.

Continued: Federal Information Security Management Act Audit Fiscal Year 2014

Rec. #		
11	<i>Finding</i>	<u>Vulnerability Scanning</u> - We were told in an interview that OPM performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2014.
	<i>Recommendation</i>	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for detecting and vulnerabilities.
12	<i>Finding</i>	<u>Vulnerability Scanning</u> - The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<i>Recommendation</i>	The OIG recommends that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for tracking and remediating vulnerabilities.
14	<i>Finding</i>	<u>Patching Management</u> - Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	<i>Recommendation</i>	The OIG recommends the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for keeping information systems up-to-date with patches and service packs.

Continued: Federal Information Security Management Act Audit Fiscal Year 2014

Rec. #		
21	<i>Finding</i>	<u>Multi-factor Authentication</u> - OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by FY 2012. However, as of the end of the FY 2014, none of the 47 major systems at OPM require PIV authentication.
	<i>Recommendation</i>	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for authenticating to information systems.
23	<i>Finding</i>	<u>Test of Security Controls</u> - FISMA requires agencies to test the security controls of all of their systems on an annual basis. In FY 2014, 10 systems were not subject to adequate security control tests.
	<i>Recommendation</i>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	<i>Status</i>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
24	<i>Finding</i>	<u>Contingency Plans</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. We received updated contingency plans for 41 out of 47 information systems on OPM's master system inventory.
	<i>Recommendation</i>	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.
	<i>Status</i>	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for recovering from an unplanned system outage.

Continued: Federal Information Security Management Act Audit Fiscal Year 2014

Rec. #		
25	<i>Finding</i>	<u>Contingency Plan Testing</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2014, eight were not subject to adequate contingency plan tests.
	<i>Recommendation</i>	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.
	<i>Status</i>	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for recovering from an unplanned system outage.
28	<i>Finding</i>	<u>Contractor System Documentation</u> - The OCIO maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, many of the documented ISAs have expired.
	<i>Recommendation</i>	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.
29	<i>Finding</i>	<u>Contractor System Documentation</u> - While the OCIO tracks ISAs, it does not track Memorandums of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. We were told that program offices were responsible for maintaining MOU/As. While we have no issue with the program offices maintaining the memorandums, the OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.
	<i>Recommendation</i>	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.

Title: Flash Audit: OPM's Infrastructure Improvement Project
Report #: 4A-CI-00-15-055
Date: June 17, 2015

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

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

Rec. #		
1	Finding	<u>Security Controls Self-Assessment</u> – Retirement Services (RS) did not conduct a security controls self-assessment in 2014, as required by OPM policy.
	Recommendation	The OIG recommends that RS ensure that the AHBOSS security controls are tested on an annual basis in accordance with OPM policy.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and remediating security vulnerabilities on the system.

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

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

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

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

Title: Audit of Information Security Controls @ OPM's GP Plateau Baseline 6 Learning Management System
Report #: 4A-HR-00-15-015
Date: July 31, 2015

Rec. #		
4	Finding	<u>Privacy Impact Assessment</u> – HRS completed a Privacy Threat Analysis (PTA) during April 2014 and determined that a PIA was required for the system, but they have not yet completed a PIA in accordance with the E-Government Act of 2002.
	Recommendation	The OIG recommends that HRS complete a current Privacy Impact Assessment for the GPB6 LMS.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying privacy vulnerabilities existing on the information system.
6	Finding	<u>Updated POA&M Documentation</u> – We noted 60 weaknesses on the POA&M that had a status of delayed, but had no updated completion date, as required by OPM'S POA&M SOP.
	Recommendation	The OIG recommends that HRS update the GPB LMS POA&M to include a new scheduled completion date for all delayed items.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for maintaining and documenting POA&M's.

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

Rec. #		
2	Finding	<u>SDLC Methodology</u> - OPM has a history of troubled system development projects. In our opinion, the root cause of these issues relates to the lack of central policy and oversight of systems development.
	Recommendation	The OIG continues to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy to all of OPM's system development projects.
	Status	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring stability of systems development projects.
3	Finding	<u>Security Assessment and Authorization</u> – Eleven OPM systems are operating without an active Security Assessment and Authorization.
	Recommendation	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
4	Finding	<u>Security Assessment and Authorization</u> – Several OPM systems are operating without an active Security Assessment and Authorization. In our opinion, one root cause of this issue relates to the lack of accountability for system owners that fail to subject their systems to the Authorization process.
	Recommendation	The OIG recommends that the performance standards of all OPM system owners be modified to include a requirement related to FISMA compliance for the information systems they own. At a minimum, system owners should be required to ensure that their systems have valid Authorizations.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
Rec. #		
7	Finding	<u>Test of Security Controls</u> - FISMA requires agencies to test the security controls of all of its systems on an annual basis. In FY 2015, 16 systems were not subject to adequate security control tests.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.

Continued: Federal Information Security Management Act Audit Fiscal Year 2015

Rec. #		
8	<i>Finding</i>	<u>Baseline Configurations</u> - In FY 2015, OPM has continued its efforts toward formalizing baseline configurations for critical applications, servers, and workstations. The OCIO had established baselines for several operating systems, but not for all that the agency uses in its environment.
	<i>Recommendation</i>	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, ██████, ██████, ██████, and ██████.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring that information systems are initially configured in a secure manner.
9	<i>Finding</i>	<u>Configuration Auditing</u> - There are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.
	<i>Recommendation</i>	The OIG recommends the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 7 has been completed.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring that servers are in compliance with approved security settings.
10	<i>Finding</i>	<u>Vulnerability Scanning</u> - We were told in an interview that OPM performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2014.
	<i>Recommendation</i>	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for detecting and remediating vulnerabilities.

Continued: Federal Information Security Management Act Audit Fiscal Year 2015

Rec. #		
11	<i>Finding</i>	<u>Vulnerability Scanning</u> - The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<i>Recommendation</i>	The OIG recommends that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for tracking and remediating vulnerabilities.
13	<i>Finding</i>	<u>Unsupported Software</u> - The results of our vulnerability scans indicated that OPM's production environment contains severely out-of-date and unsupported software and operating platforms.
	<i>Recommendation</i>	The OIG recommends the OCIO implement a process to ensure that only supported software and operating platforms are utilized within the network environment.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring up-to-date software and operating platforms.
14	<i>Finding</i>	<u>Patching Management</u> - Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	<i>Recommendation</i>	The OIG recommends the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for keeping information systems up-to-date with patches and service packs.

Continued: Federal Information Security Management Act Audit Fiscal Year 2015

Rec. #		
16	Finding	<u>Multi-factor Authentication</u> - OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by FY 2012. However, as of the end of the FY 2014, none of the 47 major systems at OPM require PIV authentication.
	Recommendation	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.
18	Finding	Agency-wide Risk Management - the OCIO organized a Risk Executive Function comprised of several IT security professionals. However, the 12 primary elements of the Risk Executive Function as described in NIST SP 800-39 were not all fully implemented.
	Recommendation	The OIG recommends that the OCIO continue to develop its Risk Executive Function to meet all of the intended requirements outlined in NIST SP 800-39, section 2.3.2 Risk Executive (Function).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security risks at OPM.
24	Finding	<u>Contingency Plans</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. We received updated contingency plans for 41 out of 47 information systems on OPM’s master system inventory.
	Recommendation	The OIG recommends that the OCIO ensure that all of OPM’s major systems have contingency plans in place and are reviewed and updated annually.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

Continued: Federal Information Security Management Act Audit Fiscal Year 2015

Rec. #		
25	Finding	<u>Contingency Plan Testing</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. In FY 2014, eight were not subject to adequate contingency plan tests.
	Recommendation	The OIG recommends that OPM’s program offices test the contingency plans for each system on an annual basis. The contingency plans should be tested for the systems that were not subject to adequate testing in FY 2014 as soon as possible.
	Status	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.
26	Finding	<u>Contractor System Documentation</u> - The OCIO maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, many of the documented ISAs have expired.
	Recommendation	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.
27	Finding	<u>Contractor System Documentation</u> - While the OCIO tracks ISAs, it does not track Memorandums of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. We were told that program offices were responsible for maintaining MOU/As. While we have no issue with the program offices maintaining the memorandums, the OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.
	Recommendation	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.

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

Rec. #		
1	Finding	<u>Major IT Business Case</u> – OPM completed a Business Case for its infrastructure improvement project. However, OPM officials failed to perform almost all of the capital planning activities that are required to be associated with a Business Case document.
	Recommendation	The OIG recommends that OPM complete an Analysis of Alternatives as described in the Capital Programming Guide supplement to OMB Circular A-11 as soon as possible. This analysis should recognize changes in the internal and external environment and no consideration should be given to funds already spent associated with the Project (i.e., avoid the sunk cost fallacy).
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for minimizing the risk of a major project failure.
2	Finding	<u>Lifecycle Cost Estimates</u> - OPM's Business Case submitted to OMB with the FY 2017 budget request outlines the costs already incurred for this Project along with reasonable short-term cost estimates to finish developing the IaaS portion. However, its cost estimates for modernizing and migrating its information systems to the new environment are unsubstantiated because of the incomplete inventory and technical analysis.
	Recommendation	The OIG recommends that OPM leverage the application profiling scoring framework to develop cost estimates for modernizing and/or migrating all OPM information systems, and use this information to support the capital planning activities referenced in Recommendation 1. The Business Case should be continuously updated to reflect these cost estimates as they become more concrete.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for minimizing the risk of a major project failure.

Title: Web Application Security Review
Report #: 4A-CI-00-16-061
Date: October 31, 2016

Rec. #		
1	Finding	<u>Web Application Inventory</u> - OPM does not maintain an adequate inventory of web applications. OPM's OCIO has developed an inventory of servers, databases, and network devices, but the inventory does not identify the purpose, role, or owner of each device.
	Recommendation	The OIG recommends that OPM create a formal and comprehensive inventory of web applications. The inventory should identify which applications are public facing and contain personally identifiable information or sensitive agency information, identify the application owner, and itemize all system interfaces with the web application.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for identifying and documenting web based applications.
2	Finding	<u>Policies and Procedures</u> - OPM maintains information technology (IT) security policies and procedures that address NIST SP 800-53 security controls. OPM also maintains system development policies and standards. While these policies, procedures, and standards apply to all IT assets, they are written at a high level and do not address some critical areas specific to web application security and development.
	Recommendation	The OIG recommends that OPM create or update its policies and procedures to provide guidance specific to the hardening of web server operating systems and the secure design and coding of web-based applications.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for establishing policy and procedures governing the hardening of web applications.
3	Finding	<u>Web Application Vulnerability Scanning</u> - While the OCIO was able to provide historical server vulnerability scan results, we were told that there is not a formal process in place to perform routine credentialed web application vulnerability scans (however, ad-hoc non-credentialed scans were performed).
	Recommendation	The OIG recommends that OPM implement a process to perform credentialed web application vulnerability scans and track any identified vulnerabilities until they are remediated.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for detecting and tracking vulnerabilities.

<i>Continued: Web Application Security Review</i>		
Rec. #		
4	<i>Finding</i>	<u>Web Application Vulnerability Scanning</u> - The results of the credentialed web application scans that we performed during this review indicate that several applications and the servers hosting these applications contain security weaknesses.
	<i>Recommendation</i>	The OIG recommends that OPM analyze our scan results to identify false positives and remediate any verified vulnerabilities.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for remediating vulnerabilities.

Title: Federal Information Security Management Act Audit Fiscal Year 2016		
Report #: 4A-CI-00-16-039		
Date: November 10, 2015		
Rec. #		
1	<i>Finding</i>	<u>Security Management Structure</u> – OPM has experienced a high turnover rate for ISSO and CISO positions and has struggled to backfill these vacancies.
	<i>Recommendation</i>	The OIG recommends that OPM hire a sufficient number of ISSOs to adequately support all of the agency’s major information systems.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for managing information security.
3	<i>Finding</i>	<u>SDLC Methodology</u> - OPM has a history of troubled system development projects. In our opinion, the root cause of these issues relates to the lack of central policy and oversight of systems development.
	<i>Recommendation</i>	We continue to recommend that the OCIO develop a plan and timeline to enforce the new SDLC policy on all of OPM’s system development projects.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring stability of systems development projects.

Continued: Federal Information Security Management Act Audit Fiscal Year 2016

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

Continued: Federal Information Security Management Act Audit Fiscal Year 2016

Rec. #		
8	Finding	<u>Adherence to Remediation Deadlines</u> – Of OPM’s 46 major information systems, 43 have POA&M items that are greater than 120 days overdue. Further, 85% of open POA&Ms are over 30 days overdue and over 78% are over 120 days overdue.
	Recommendation	The OIG recommends that OPM adhere to remediation dates for its POA&M weaknesses.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing POA&M weakness remediation.
9	Finding	<u>Contractor System Documentation</u> - The OCIO maintains a separate spreadsheet documenting interfaces between OPM and contractor-operated systems and the related Interconnection Security Agreements (ISA). However, many of the documented ISAs have expired.
	Recommendation	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.
10	Finding	<u>Contractor System Documentation</u> - While the OCIO tracks ISAs, it does not track Memorandums of Understanding/Agreement (MOU/A). These documents outline the terms and conditions for sharing data and information resources in a secure manner. We were told that program offices were responsible for maintaining MOU/As. While we have no issue with the program offices maintaining the memorandums, the OCIO should track MOU/As to ensure that valid agreements are in place for each documented ISA.
	Recommendation	The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.

Continued: Federal Information Security Management Act Audit Fiscal Year 2016

Rec. #		
11	Finding	<u>System Inventory</u> – OPM’s system inventory lists the devices and software in the environment, but does not describe the specific servers the software resides on or the information systems the devices and software support.
	Recommendation	The OIG recommends that OPM improve its system inventory by correlating the elements of the inventory to the servers and information systems they reside on.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for oversight, risk management, and securing the agency’s information systems.
12	Finding	<u>Baseline Configurations</u> - In FY 2016, OPM has continued its efforts toward formalizing baseline configurations for critical applications, servers, and workstations. The OCIO had established baselines for several operating systems, but not for all that the agency uses in its environment.
	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, ██████, ██████, ██████ and ██████
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that information systems are initially configured in a secure manner.
13	Finding	<u>Document Deviations to the Standard Configuration Baseline</u> – OPM does not maintain a record of the specific deviations from generic configuration standards.
	Recommendation	Where an OPM configuration standard is based on a pre-existing generic standard, The OIG recommends that OPM document all instances where the OPM-specific standard deviates from the recommended configuration setting.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for effectively auditing a system’s actual settings.

Continued: Federal Information Security Management Act Audit Fiscal Year 2016

Rec. #		
14	<i>Finding</i>	<u>Vulnerability Scanning</u> - We were told in an interview that OPM performs monthly vulnerability scans using automated scanning tools. However, we have been unable to obtain tangible evidence that vulnerability scans have been routinely conducted for all OPM servers in FY 2016.
	<i>Recommendation</i>	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for detecting and remediating vulnerabilities.
15	<i>Finding</i>	<u>Unsupported Software</u> - The results of our vulnerability scans indicated that OPM's production environment contains severely out-of-date and unsupported software and operating platforms.
	<i>Recommendation</i>	The OIG recommends the OCIO implement a process to ensure that only supported software and operating platforms are used within the network environment.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring up-to-date software and operating platforms.
16	<i>Finding</i>	<u>Configuration Auditing</u> - There are several operating platforms used by OPM that do not have documented and approved baselines. Without approved baseline configurations these systems cannot be subject to an adequate compliance audit.
	<i>Recommendation</i>	The OIG recommends the OCIO conduct routine compliance scans against established baseline configurations for all servers and databases in use by OPM. This recommendation cannot be addressed until Recommendation 13 has been completed.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for ensuring that servers are in compliance with approved security settings.

Continued: Federal Information Security Management Act Audit Fiscal Year 2016

Rec. #		
17	<i>Finding</i>	<u>Vulnerability Scanning</u> - The OCIO does not centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<i>Recommendation</i>	The OIG recommends that the OCIO implement a process to centrally track the current status of security weaknesses identified during vulnerability scans to remediation or risk acceptance.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for tracking and remediating vulnerabilities.
18	<i>Finding</i>	<u>Patching Management</u> - Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.
	<i>Recommendation</i>	The OIG recommends the OCIO implement a process to apply operating system and third party vendor patches in a timely manner, which is defined within the OPM Information Security and Privacy Policy Handbook.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for keeping information systems up-to-date with patches and service packs.
19	<i>Finding</i>	<u>Contractor Access Termination</u> – OPM does not maintain a complete list of the contractors with access to OPM’s network and the termination process for contractors is de-centralized.
	<i>Recommendation</i>	The OIG recommends that the OCIO maintain a centralized list of all contractors that have access to the OPM network and use this list to routinely audit all user accounts for appropriateness.
	<i>Status</i>	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	Improved controls for managing appropriate access to information systems.

Continued: Federal Information Security Management Act Audit Fiscal Year 2016

Rec. #		
20	Finding	<u>Multi-factor Authentication</u> - OMB Memorandum M-11-11 required all federal information systems to be upgraded to use PIV credentials for multi-factor authentication by FY 2012. However, as of the end of the FY 2016, none of the 46 major systems at OPM require PIV authentication.
	Recommendation	The OIG recommends that the OCIO meet the requirements of OMB M-11-11 by upgrading its major information systems to require multi-factor authentication using PIV credentials.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for authenticating to information systems.
21	Finding	<u>Specialized IT Security Training</u> – Only 73% of employees required to take specialized security training did so in FY 2016.
	Recommendation	The OIG recommends that the OCIO ensure that all employees with significant information security responsibility take meaningful and appropriate specialized security training on an annual basis.
	Status	This recommendation was closed after September 30, 2017
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for managing information security risks at OPM.
23	Finding	<u>Test of Security Controls</u> - FISMA requires agencies to test the security controls of its systems on an annual basis. In FY 2017, 16 systems were not subject to adequate security control tests.
	Recommendation	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
25	Finding	<u>Contingency Plans</u> – FISMA requires that a contingency plan be in place for each major application, and that the contingency plan be tested on an annual basis. We received updated contingency plans for 41 out of 47 information systems on OPM’s master system inventory.
	Recommendation	The OIG recommends that the OCIO ensure that all of OPM’s major systems have contingency plans in place and are reviewed and updated annually.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for recovering from an unplanned system outage.

Continued: Federal Information Security Management Act Audit Fiscal Year 2016

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

Title: Audit of Information Security Controls @ OPM’s FACES

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

Date: November 21, 2016

Rec. #		
1	Finding	<u>Security Assessment and Authorization</u> – The prior authorization for FACES expired in January 2015, and the system does not have a valid Authorization as of the date of this report.
	Recommendation	The OIG recommends that OPM complete a current Security Assessment and Authorization for FACES.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that risk has been assessed before being approved to operate.
Rec. #		
2	Finding	<u>System Security Plan</u> – The most recent SSP for FACES does not include controls that were added to the current revision of NIST SP 800-53 (Revision 4).
	Recommendation	The OIG recommends that OPM update the FACES SSP in accordance with the agency’s policies and NIST standards.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that system security controls are properly documented.

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

Rec. #		
3	Finding	<u>Security Controls Continuous Monitoring</u> – The documentation for 2014 and 2015 indicates that the FACES system was not subject to adequate security control testing in those years. Furthermore, there have not been any security control tests completed for FACES since April 2015.
	Recommendation	The OIG recommends that OPM ensure that the FACES security controls are continuously monitored in accordance with the agency’s policy.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
5	Finding	<u>Privacy Impact Assessment</u> – OPM policy requires system owners to conduct a PIA every three years for existing systems even when there are no changes to the system. The most recent PIA for FACES was conducted in October of 2012.
	Recommendation	The OIG recommends that OPM ensure that a PIA is conducted for FACES in accordance with OPM policy.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for protecting personally identifiable information maintained by the system.
6	Finding	<u>Plan of Action and Milestones Process</u> - Many of the security weaknesses discovered during continuous monitoring activities for FACES were not added to the system’s POA&M.
	Recommendation	The OIG recommends that OPM add a POA&M entry for all known weaknesses of FACES.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for addressing weaknesses in a timely manner and limiting system exposure to malicious attacks.
7	Finding	<u>Action plan for Overdue POA&M Items</u> - 20 of the 25 items on the FACES POA&M were over 200 days overdue.
	Recommendation	The OIG recommends that OPM develop a detailed action plan to remediate all overdue POA&M items. This action plan should include realistic estimated completion dates.
	Status	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	Improved controls for addressing weaknesses in an appropriate timeframe and limiting system exposure to malicious attacks.

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

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

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

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

III. EXPERIENCE-RATED INSURANCE AUDITS

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

Title: Global Audit of Coordination of Benefits for BCBS Plans		
Report #: 1A-99-00-14-046		
Date: July 29, 2015		
Rec. #		
5	Finding	<u>Statistical Review of Incorrectly Coordinated Claims</u> – For certain claims where there were a large number of claims with small payments, the OIG used a statistical sampling methodology to determine the incorrect payment. We projected the sample results to the relevant universe of paid claims and estimate that the BCBS plans incorrectly paid \$4,486,775 in claims that were not properly coordinated with Medicare.
	Recommendation	The OIG recommends that the OPM contracting officer disallow \$4,486,775 for claims that were not paid in good faith and unreasonably charged to the FEHBP.
	Status	OPM is still reviewing this recommendation. As of September 30, 2017, no money has been collected and there was a receivable of \$4,486,775.
	Estimated Program Savings	Total Savings when Implemented: \$4,486,775
	Other Nonmonetary Benefit	N/A

Title: Audit of Health Care Service Corporation		
Report #: 1A-10-17-14-037		
Date: November 19, 2015		
Rec. #		
1	Finding	<u>Veteran Affairs Claim Review</u> - Our review determined HCSC incorrectly paid 13,108 VA claims, resulting in overcharges of \$35,562,962 to the FEHBP. For most of these claims, the Plan did not provide documentation to support how the Plan determined that paying these claims using billed charges was cost effective and advantageous to the FEHBP
	Recommendation	We recommend that the contracting officer disallow \$35,562,962 for claim overcharges and verify that the Plan returns all amounts recovered to the FEHBP. Due to the nature of this finding and the substantial amount questioned, we also recommend that the contracting officer contact the Illinois, Montana, and New Mexico VA service areas to discuss a practical approach for recovery of these claims. Based on regulations, the contracting office should not allow the Plan to offset these recoveries against future payments.
	Status	OPM agreed with \$35,560,326 and disagreed with \$2,636. As of September 30, 2017, \$664,072 had been collected and there was a receivable of \$34,896,254.
	Estimated Program Savings	Total Savings when Implemented: \$35,560,326
	Other Nonmonetary Benefit	N/A

Continued: Audit of Health Care Service Corporation

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

Title: Global Audit of BCBS Claims-to-Enrollment Match
Report #: 1A-99-00-15-008
Date: January 21, 2016

Rec. #		
1	Finding	<u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claim lines, resulting in overcharges of \$10,051,009 to the FEHBP. These claims should not have been paid because these patients were not enrolled in the FEHBP during the patient's dates of service.
	Recommendation	We recommend that the contracting officer disallow \$10,051,009 for claim overpayments and verify that the BCBS plans return all amounts recovered to the FEHBP, regardless of the Plans' ability to recover the claim payments from providers.
	Status	OPM agreed with \$8,183,315 and disagreed with \$1,867,694. As of September 30, 2017, \$5,311,665 has been collected and there was a receivable for \$2,871,650.
	Estimated Program Savings	Total Savings when Implemented: \$8,183,315
	Other Nonmonetary Benefit	N/A
3	Finding	<u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claim lines, resulting in overcharges of \$10,051,009 to the FEHBP. Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.
	Recommendation	We recommend that the contracting officer require the Association to perform a cost analysis to determine the benefit of automating the process of updating the FEP Express system when enrollment discrepancies are identified between the FEP OC and employing agencies. If determined cost effective, we recommend that the contracting officer require the Association to implement these automated procedures.
	Status	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	Estimated Program Savings	Unknown – however, improved system controls for updating enrollment records should result in increased program savings.
	Other Nonmonetary Benefit	Improved controls over processing claims for only eligible members.
4	Finding	<u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claim lines, resulting in overcharges of \$10,051,009 to the FEHBP. Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.
	Recommendation	We recommend that the contracting officer require the Association to implement a process to identify ineligible members who were terminated due to fraud or intentional misrepresentation of information yet continued to improperly file claims (e.g., medical or pharmacy). This process should be performed on a monthly basis, and the members identified should be reported to the OPM OIG Office of Investigations.
	Status	The agency informed the OIG that as of September 30, 2017, a corrective action plan is in place to address this recommendation and that corrective actions are in progress.
	Estimated Program Savings	Unknown – however, improved system controls for updating enrollment records should result in increased program savings.
	Other Nonmonetary Benefit	Improved controls for reporting fraud and/or abuse due to enrollment misrepresentation.

<i>Continued: Global Audit of BCBS Claims-to-Enrollment Match</i>		
Rec. #		
6	<i>Finding</i>	<u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claim lines, resulting in overcharges of \$10,051,009 to the FEHBP. Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.
	<i>Recommendation</i>	We recommend that the contracting officer require the Association to enhance the FEP Express system by adding an edit that defers claims where a patient's enrollment is incomplete or who has coverage under another FEP member number. In addition, the FEP Express system should defer all claims for members whose enrollment file contains inconsistencies, and not allow payment on these claims until the member's enrollment file is properly updated. This edit should contain a unique deferral code that cannot be overridden by claims processors.
	<i>Status</i>	This recommendation was closed after September 30, 2017.
	<i>Estimated Program Savings</i>	Unknown – however, improved system controls should result in increased program savings.
	<i>Other Nonmonetary Benefit</i>	Improved controls over processing claims for only eligible members.
8	<i>Finding</i>	<u>Statistical Review of Member Enrollment Issues</u> – For certain claims where there were a large number of claims with small payments, we used a statistical sampling methodology to determine the incorrect payment. We projected the sample results to the relevant universe of paid claims. We are 95 percent confident that BCBS plans incorrectly paid \$3,207,289 in claims paid to ineligible members.
	<i>Recommendation</i>	We recommend that the contracting officer disallow \$3,207,289 for claims that were not paid in good faith and unreasonably charged to the FEHBP.
	<i>Status</i>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<i>Estimated Program Savings</i>	Total Savings when Implemented: \$3,207,289
	<i>Other Nonmonetary Benefit</i>	Approving of statistical sampling, results in a long term standard practice to perform additional statistical reviews.

Title: Global Audit of OBRA 90 for BCBS Plans
Report #: 1A-99-00-15-047
Date: June 17, 2016

Rec. #		
1	Finding	<u>Global Omnibus Budget Reconciliation Act of 1990</u> – Our review of high dollar claims that were subject to or potentially subject to the OBRA 90 pricing guidelines determined that the BCBS plans overpaid 686 of these claims by \$10,792,073.
	Recommendation	We recommend that the contracting officer disallow \$10,792,073 for claim overpayments and verify that the BCBS plans return all amounts recovered to the FEHBP.
	Status	OPM agreed with \$9,683,969 and disagreed with \$1,108,104. As of September 30, 2017, \$8,272,667 had been collected and there was a receivable of \$1,411,302.
	Estimated Program Savings	Total Savings when Implemented: \$9,683,969
	Other Nonmonetary Benefit	N/A
3	Finding	<u>Global Omnibus Budget Reconciliation Act of 1990</u> – Our review determined that 81 claims were questioned due to FEP Express system processing errors, resulting in net overcharges of \$2,225,093 to the FEHBP. In most instances, the claims bypassed OBRA 90 pricing edits in the FEP Express system due to the fact that [REDACTED]. Our review determined that if the FEP Express system had identified that an invalid Medicare provider number was on file during the processing of these claims, the OBRA 90 allowance would have been properly applied.
	Recommendation	We recommend that the contracting officer require the Association to enhance the FEP Express system by adding an edit that automatically defers claims where [REDACTED] when being automatically priced as OBRA 90. If determined cost effective, the contracting officer should ensure the Association implements an automated process to utilize the Medicare provider number files issued by CMS.
	Status	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	Estimated Program Savings	Unknown – however, improved processes should result in increased program savings.
	Other Nonmonetary Benefit	Improved systematic process for accurately pricing OBRA 90 claims.

<i>Continued: Global Audit of OBRA 90 for BCBS Plans</i>		
Rec. #		
4	<i>Finding</i>	Global Omnibus Budget Reconciliation Act of 1990 – Our review determined that 418 claims were priced with outdated Medicare effective rates, resulting in net overcharges of \$2,911,375 to the FEBHP. At the time these claims were priced, the FEP Express system had not been updated with the most recent Center for Medicare and Medicaid Services (CMS) pricing rates. Although the FEP Express system is updated annually with the CMS effective rates, the system is not updated when CMS releases monthly or quarterly pricing changes, which in this case would have resulted in savings to the FEHBP.
	<i>Recommendation</i>	Due to the ongoing savings identified year after year with the FEP OC using monthly and/or quarterly CMS pricing releases, we recommend that the contracting officer require the Association to perform a risk analysis to determine if it is cost effective to implement a process to include CMS pricing updates in the FEP Express system at the time the updates are released.
	<i>Status</i>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<i>Estimated Program Savings</i>	Unknown – however, improved processes should result in increased program saving.
	<i>Other Nonmonetary Benefit</i>	Improved systematic process for accurately pricing OBRA 90 claims.

Title: Global Audit of Coordination of Benefits		
Report #: 1A-99-00-15-060		
Date: October 13, 2016		
Rec. #		
1	<i>Finding</i>	Global Coordination of Benefits with Medicare Review - BCBS plans incorrectly paid 5,070 claim lines, resulting in overcharges of \$2,986,416 to the FEHBP. These claims should not have been paid because these patients Medicare was primary during the patient's dates of service.
	<i>Recommendation</i>	We recommend that the contracting officer disallow \$2,986,416 for claim overpayments and verify that the BCBS plans return all amounts recovered to the FEHBP.
	<i>Status</i>	OPM agreed with \$2,575,018 and disagreed with \$411,398. As of September 30, 2017, \$1,632,121 had been collected and there was a receivable of \$942,897.
	<i>Estimated Program Savings</i>	Total Savings when Implemented: \$2,575,018
	<i>Other Nonmonetary Benefit</i>	N/A

<i>Continued: Global Audit of Coordination of Benefits</i>		
Rec. #		
3	Finding	<u>Statistical Review of Incorrectly Coordinated Claims</u> – For certain claims where there were a large number of claims with small payments, we used a statistical sampling methodology to determine the incorrect payment. We projected the sample results to the relevant universe of paid claims. We are 95 percent confident that BCBS plans incorrectly paid \$3,415,424 in claims not properly coordinated with Medicare.
	Recommendation	We recommend that the contracting officer disallow \$3,415,424 for claims that were not paid in good faith and unreasonably charged to the FEHBP.
	Status	OPM is still reviewing this recommendation. As of September 30, 2017, no money has been collected and there was a receivable of \$3,415,424
	Estimated Program Savings	Total Savings when Implemented:\$3,415,424
	Other Nonmonetary Benefit	Approving of statistical sampling, results in a long term standard practice to perform additional statistical reviews.

Title: Audit of BlueCross BlueShield of North Carolina		
Report #: 1A-10-33-15-009		
Date: November 10, 2016		
Rec. #		
1	Finding	<u>Veteran Affairs Claims Review</u> - Our review determined that the Plan incorrectly paid 10,622 claims to VA service providers, resulting in overcharges of \$17,652,501 to the FEHBP.
	Recommendation	We recommend that the contracting officer disallow \$17,652,501 for claim overcharges and verify that the Plan returns all amounts to the FEHBP. Due to regulations, the contracting office should not allow the Plan to offset any recoveries against future payments, unless approved by a VA official.
	Status	OPM is still reviewing this recommendation. As of September 30, 2017, no money has been collected and there was a receivable of \$17,652,501.
	Estimated Program Savings	Total Savings when Implemented: \$17,652,501
	Other Nonmonetary Benefit	N/A

Continued: Audit of BlueCross BlueShield of North Carolina

Rec. #		
2	<i>Finding</i>	<u>Veteran Affairs Claims Review</u> - We reviewed a sample of claims where the amount paid to U.S. Department of Veterans Affairs (VA) service providers was greater than or equal to the amount billed by the provider. We consider these claims as high risk for payment errors because paying a claim at or above the billed amount could indicate that the FEHBP did not receive a discount in the pricing of that claim.
	<i>Recommendation</i>	We recommend that the contracting officer require the Plan to perform a cost analysis using all LOBs and types of services (i.e., inpatient, outpatient, and physician) to determine what rates are reasonable for the FEHBP to obtain and pay VA facilities. Based on this analysis, we recommend the contracting officer provide oversight that the Plan practices due diligence to ensure the Plan contracts equitably to pay VA claims on behalf of the FEHBP.
	<i>Status</i>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<i>Estimated Program Savings</i>	Unknown – however, improving provider contracted rates should result in increased program savings to health benefit charges, administrative cost and member’s cost share for health benefit services.
	<i>Other Nonmonetary Benefit</i>	Improved controls over ensuring VA claims are processed appropriately.
3	<i>Finding</i>	<u>Veteran Affairs Claims Review</u> - We reviewed a sample of claims where the amount paid to U.S. Department of Veterans Affairs (VA) service providers was greater than or equal to the amount billed by the provider. We consider these claims as high risk for payment errors because paying a claim at or above the billed amount could indicate that the FEHBP did not receive a discount in the pricing of that claim.
	<i>Recommendation</i>	We recommend that the contracting officer require the Plan to perform an analysis to determine the extent that the Plan’s administrative cost reimbursements were overstated as a result of the overpayment of VA claims. The contracting officer should ensure that the Plan returns all excessive administrative cost reimbursements to the FEHBP.
	<i>Status</i>	OPM is still reviewing this recommendation. No corrective actions have been implemented at this time.
	<i>Estimated Program Savings</i>	Unknown – however, improving provider contracted rates should result in increased program savings to health benefit charges, administrative cost and member’s cost share for health benefit services.
	<i>Other Nonmonetary Benefit</i>	Improved controls over ensuring VA claims are processed appropriately.

<i>Continued: Audit of BlueCross BlueShield of North Carolina</i>		
Rec. #		
4	<i>Finding</i>	<u>Hospice Claims Review</u> – Our review determined that the Plan incorrectly paid 833 claims for Hospice services, resulting in overcharges of \$964,834 to the FEHBP.
	<i>Recommendation</i>	We recommend that the contracting officer disallow \$964,834 for claim overcharges and verify that the Plan returns all amounts recovered to the FEHBP.
	<i>Status</i>	OPM agreed with \$964,834. As of September 30, 2017, \$477,658 had been collected and there was a receivable of \$487,176.
	<i>Estimated Program Savings</i>	Total Savings when Implemented: \$964,834
	<i>Other Nonmonetary Benefit</i>	N/A
5	<i>Finding</i>	<u>Indian Health Claims Review</u> - Our review determined that the Plan incorrectly paid 135 claims to Indian Health service providers, resulting in overcharges of \$26,140 to the FEHBP.
	<i>Recommendation</i>	We recommend that the contracting officer disallow \$26,140 for claim overcharges and verify that the Plan returns all amounts recovered to the FEHBP.
	<i>Status</i>	OPM agreed with \$26,140. As of September 30, 2017, \$16,648 had been collected and there was a receivable of \$9,492.
	<i>Estimated Program Savings</i>	Total Savings when Implemented: \$26,140
	<i>Other Nonmonetary Benefit</i>	N/A
6	<i>Finding</i>	<u>System Pricing Review</u> – Our review indicated that the Plan incorrectly paid two claims where the FEHBP paid as primary insurer, resulting in overcharges of \$5,022 to the FEHBP.
	<i>Recommendation</i>	We recommend that the contracting officer disallow \$5,022 for claim overcharges and verify that the Plan returns all amounts recovered to the FEHBP.
	<i>Status</i>	OPM agreed with \$5,022. As of September 30, 2017, \$3,128 had been collected and there was a receivable of \$1,894.
	<i>Estimated Program Savings</i>	Total Savings when Implemented: \$5,022
	<i>Other Nonmonetary Benefit</i>	N/A

IV. COMMUNITY-RATED INSURANCE AUDITS

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

Title: Audit of Independent Health Report #: 1C-QA-00-14-045 Date: August 12, 2015		
Rec. #		
1	Finding	<p><u>Defective Pricing</u> - The Certificate of Accurate Pricing Independent Health (Plan) signed for contract year 2012 was defective. In accordance with Federal regulations, the FEHBP is therefore due a rate reduction for this year. Application of the defective pricing remedy shows that the FEHBP is due a premium adjustment of \$8,969,710.</p> <p>The OIG determined that defective pricing existed in 2012 because the Plan selected an incorrect SSSG and, consequently, failed to apply the largest SSSG discount to the FEHBP. We also found the Plan did not appropriately credit the FEHBP rates for a state assessment that was included in its community rates.</p>
	Recommendation	The OIG recommends that the OPM contracting officer require the Plan to return \$8,969,710 to the FEHBP for defective pricing in contract year 2012.
	Status	The agency agreed with the recommendation. The last update the OIG received was that as of August 4, 2017, there was a receivable of \$8,828,534.
	Estimated Program Savings	Total savings when implemented: \$8,828,534
	Other Nonmonetary Benefit	To ensure that Federal employees and their employing agencies are paying a fair and reasonable price for health coverage.
2	Finding	<p><u>Lost Investment Income</u> - In accordance with the FEHBP regulations and the contract between OPM and the Plan, the FEHBP is entitled to recover lost investment income on the defective pricing finding in contract year 2012. The OIG determined that the FEHBP is due \$526,970 for lost investment income, calculated through July 31, 2015.</p>
	Recommendation	The OIG recommends that the OPM contracting officer require the Plan to return \$526,970 to the FEHBP for lost investment income, calculated through July 31, 2015. We also recommend that the OPM contracting officer recover lost investment income on amounts due for the period beginning August 1, 2015, until all defective pricing amounts have been returned to the FEHBP.
	Status	OPM agreed with the recommendation. The last update the OIG received was that as of August 4, 2017, there was a receivable of \$904,926 (lost investment income will continue to accrue until OPM is repaid).
	Estimated Program Savings	Total savings when implemented: \$904,926 (plus interest since 8/1/2015)
	Other Nonmonetary Benefit	To ensure that the Federal Government receives reimbursement for interest lost on Program funds due to improper payments.

Title: Audit of HMO Health Ohio

Report #: 1C-L4-00-16-013

Date: September 23, 2016

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

Title: Audit of Aetna Open Access – Capitol Region

Report #: 1C-JN-00-16-019

Date: January 31, 2017

Rec. #		
1	Finding	<p><u>Medical Loss Ratio (MLR) Penalty Underpayment</u> - The Plan calculated an MLR of █████ percent for contract year 2013. Since this ratio was under the established threshold of 85 percent, the Plan paid a penalty to OPM of \$14,155,486. However, our audit identified additional issues that resulted in an audited MLR that was lower than that calculated by the Plan. Consequently, our audit determined that the Plan owed an additional penalty of \$16,169,511 for contract year 2013. Contributing to the additional penalty were the following factors:</p> <ul style="list-style-type: none"> - A tax allocation method that was not applied proportionately, appropriately, and was not based on a generally accepted accounting method. - The Plan’s use of a large group premium ratio to allocate various expenses that did not produce the most accurate results. - Incurred claims that were paid for non-covered benefits. - An unsupported manual pharmacy claim adjustment credit.
	Recommendation	The OIG recommends that the OPM contracting officer require the Plan to return \$16,169,511 to the MLR subsidization penalty account for contract year 2013.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	Total savings when implemented: \$16,169,511
	Other Nonmonetary Benefit	To ensure that Federal employees and their employing agencies are receiving the best value for their premium dollar by requiring plans to spend at least 85 percent of every premium dollar on claims.
4	Finding	<p><u>Medical Loss Ratio (MLR) Penalty Underpayment</u> - The Plan calculated an MLR of █████ percent for contract year 2013. Since this ratio was under the established threshold of 85 percent, the Plan paid a penalty to OPM of \$14,155,486. However, our audit identified additional issues that resulted in an audited MLR that was lower than that calculated by the Plan. Consequently, our audit determined that the Plan owed an additional penalty of \$16,169,511 for contract year 2013. Contributing to the additional penalty were the following factors:</p> <ul style="list-style-type: none"> - A tax allocation method that was not applied proportionately, appropriately, and was not based on a generally accepted accounting method. - The Plan’s use of a large group premium ratio to allocate various expenses that did not produce the most accurate results. - Incurred claims that were paid for non-covered benefits. - An unsupported manual pharmacy claim adjustment credit.
	Recommendation	The OIG recommends that the OPM contracting officer verify that the Plan has implemented internal controls to mitigate the use of incorrect and unsupported data in the MLR calculations prior to filing with OPM.
	Status	This recommendation was closed after September 30, 2017.
	Estimated Program Savings	No monetary savings, but the implementation of corrective actions will hopefully ensure that future MLR submissions are accurate and provide the best value for the health care cost charged to Federal employees and the taxpayers who subsidize the premium payments.
	Other Nonmonetary Benefit	To ensure that Federal employees and their employing agencies are receiving the best value for their premium dollar by requiring plans to spend at least 85 percent of every premium dollar on claims.

V. OTHER BENEFIT AUDITS

This section describes the open recommendations from audits of other benefit 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 any audits of Pharmacy Benefit Managements (PBMs) that participate in the FEHBP.

Title: Audit of BCBS Retail Pharmacy Member Eligibility Report #: 1H-01-00-12-072 Date: November 8, 2013		
Rec. #		
1	Finding	<u>Member Eligibility Problems Identified</u> – Because of a high error rate of potential member eligibility errors identified in a previous audit, we selected a statistical sample of member eligibility claims for 2006, 2007, and 2011 to determine if claims were properly paid. We identified 1,617 claims totaling \$680,093 that were paid by the Plan for members that were ineligible due to retroactive member eligibility changes received by the Plan after the date of the claim, making them ineligible for coverage after the claim was originally processed.
	Recommendation	The OIG recommends that the contracting officer direct the Plan to return \$680,093 to the FEHBP for eligibility errors for 2006, 2007, and 2011, as it could not document its prompt and diligent efforts to recover the overpayments.
	Status	OPM partially agreed with this recommendation. The OIG continues to have discussions with the agency concerning areas of disagreement. As of September 30, 2017, \$16,255 was recovered and there was a receivable of \$663,838.
	Estimated Program Savings	\$680,093
	Other Nonmonetary Benefit	Improved controls to verify eligible members and prevent improper payments to ineligible members.
2	Finding	<u>Member Eligibility Problems Identified</u> – Since all claims samples were selected using a statistical sampling methodology, which allows the projection of error rates identified in the samples to claims universes, we used the error rate identified for the 2011 claims sample under Recommendation #1 above and projected this rate to the 2011 claims universe. This projection questioned an additional \$681,496 in claims that were paid by the Plan for members that were ineligible due to retroactive member eligibility changes received by the Plan after the date of the claim, making them ineligible for coverage after the claim was originally processed.
	Recommendation	The OIG recommends that the contracting officer direct the Plan to return \$681,496 to the FEHBP for the projected eligibility errors for 2011.
	Status	OPM is still reviewing this recommendation.
	Estimated Program Savings	\$681,496
	Other Nonmonetary Benefit	Improved controls to verify eligible members and prevent improper payments to ineligible members.

<i>Continued: Audit of BCBS Retail Pharmacy Member Eligibility</i>		
Rec. #		
3	<i>Finding</i>	<u>Member Eligibility Problems Identified</u> – Because of a high error rate of potential member eligibility errors identified in a previous audit, we selected a statistical sample of member eligibility claims for 2006, 2007, and 2011 to determine if claims were properly paid. We identified 912 claims, totaling \$386,497 where the Plan’s claims system indicated that recoveries had not been initiated. These recoveries were not initiated due to a systemic error in the Plan’s claims system that relates to manual file corrections to a member’s eligibility file. When these types of corrections are made, the Plan’s claims system is currently unable to retroactively determine if claims were paid after the date eligibility was terminated.
	<i>Recommendation</i>	The OIG recommends that the contracting officer direct the Plan to return \$386,497 to the FEHBP for eligibility errors for 2006, 2007, and 2011, as it did not make a prompt and diligent effort to recover the overpayments.
	<i>Status</i>	OPM partially agreed with this recommendation. The OIG continues to have discussions with the agency concerning areas of disagreement. As of September 30, 2017, \$32,727 was recovered and there was a receivable of \$353,770
	<i>Estimated Program Savings</i>	\$386,497
	<i>Other Nonmonetary Benefit</i>	Improved controls to verify eligible members and prevent improper payments to ineligible members.
4	<i>Finding</i>	<u>Member Eligibility Problems Identified</u> – Since all claims samples were selected using a statistical sampling methodology, which allows the projection of error rates identified in the samples to claims universes, the OIG used the error rate identified for the 2011 claims sample under Recommendation #3 above and projected this rate to the 2011 claims universe. This projection questioned an additional \$478,133 in claims that were paid where the Plan’s claims system indicated that recoveries had not been initiated. These recoveries were not initiated due to a systemic error in the Plan’s claims system that relates to manual file corrections to a member’s eligibility file. When these types of corrections are made, the Plan’s claims system is currently unable to retroactively determine if claims were paid after the date eligibility was terminated.
	<i>Recommendation</i>	The OIG recommends that the OPM contracting officer direct the Plan to return \$478,133 to the FEHBP for projected eligibility errors for 2011.
	<i>Status</i>	OPM is still reviewing this recommendation.
	<i>Estimated Program Savings</i>	\$478,133
	<i>Other Nonmonetary Benefit</i>	Improved controls to verify eligible members and prevent improper payments to ineligible members.

<i>Continued: Audit of BCBS Retail Pharmacy Member Eligibility</i>		
Rec. #		
7	Finding	<u>Member Eligibility Problems Identified</u> – Because of a high error rate of potential member eligibility errors identified in a previous audit, we selected a statistical sample of member eligibility claims for 2006, 2007, and 2011 to determine if claims were properly paid. The OIG identified 142 claims, totaling \$49,089, which were unallowable for payment because the Plan’s claims system indicated that the member was ineligible for coverage at the date of service.
	Recommendation	The OIG recommends that the OPM contracting officer direct the Plan to return \$49,089 for contract years 2006, 2007, and 2011 to the FEHBP for eligibility errors where it did not make a prompt and diligent effort to recover the overpayments.
	Status	OPM partially agreed with this recommendation. The OIG continues to have discussions with the agency concerning areas of disagreement.
	Estimated Program Savings	\$49,089
	Other Nonmonetary Benefit	Improved controls to verify eligible members and prevent improper payments to ineligible members.
8	Finding	<u>Member Eligibility Problems Identified</u> – Since all claims samples were selected using a statistical sampling methodology, which allows the projection of error rates identified in the samples to claims universes, we used the error rate identified for the 2011 claims sample under Recommendation #7 above and projected this rate to the 2011 claims universe. This projection questioned an additional \$24,200, which were unallowable for payment because the Plan’s claims system indicated that the member was ineligible for coverage at the date of service.
	Recommendation	The OIG recommends that the OPM contracting officer direct the Plan to return \$24,200 to the FEHBP for projected eligibility errors for 2011.
	Status	OPM is still reviewing this recommendation.
	Estimated Program Savings	\$24,200
	Other Nonmonetary Benefit	Improved controls to verify eligible members and prevent improper payments to ineligible members.
11	Finding	<u>Lost Investment Income</u> – The FEHBP is due \$6,465 for LII related to the \$73,289 questioned for members who were ineligible at the time of service. We computed LII that would have been earned using the rates specified by the Secretary of Treasury.
	Recommendation	The OIG recommends that the contracting officer require the Plan to credit the FEHBP \$6,465 for LII calculated through August 31, 2013 (interest will continue to accrue after that date until all questioned costs are returned to the FEHBP).
	Status	The agency agreed with the recommendation. Final amount due for LII is contingent upon the final determination of the other findings in this audit report.
	Estimated Program Savings	\$6,465
	Other Nonmonetary Benefit	N/A

Title: Management Alert – OPM’s Procurement Process for Benefit Programs
Report #: 4A-RI-16-014
Date: October 14, 2015

Rec. #		
2	Finding	<u>Period of Performance Significantly Exceeded FAR Limits</u> - The FSAFEDS contract exceeded a 12-year period, and there were substantial changes to the Government’s program requirements that occurred over the course of the contract’s term. The FAR limits procurement for this type of service to a 5-year performance period. Furthermore, in the absence of a statutory requirement, the contract’s initial term of seven years with an unlimited number of options is adverse to the Government’s best interest because of a lack of built-in competition for enrollees that is inherent in other benefit programs administered by OPM (i.e., the Federal Employees Health Benefits Program and the Federal Employee Dental and Vision Insurance Program).
	Recommendation	The OIG recommends that controls be implemented to ensure that future program procurements follow FAR requirements and that the contracts’ periods of performance adhere to the limits under the FAR.
	Status	The agency agreed with the recommendation. The OIG has not yet received sufficient evidence that implementation has been completed.
	Estimated Program Savings	Indirect Savings -Unknown
	Other Nonmonetary Benefit	Improved controls to ensure compliance with FAR and to enhance procurements integrity within OPM.
4	Finding	Consolidation of Procurement Functions.
	Recommendation	The OIG recommends that future contracting officers assigned to these contracts not have responsibilities for administering the benefit programs, as we believe that these dual roles are a conflict of interest and will result in continued delays to future re-competitions, especially when program continuity is at risk.
	Status	The agency agreed with the recommendation. The OIG has not yet received sufficient evidence that implementation has been completed.
	Estimated Program Savings	Indirect Savings -Unknown
	Other Nonmonetary Benefit	Improved controls to ensure compliance with FAR and to enhance procurements integrity within OPM.

VI. COMBINED FEDERAL CAMPAIGN AUDITS

This section describes the open recommendations from audits of OPM's Combined Federal Campaign (CFC) Program.

Title: Audit of the Combined Federal Campaign of the National Capital Area Report #: 3A-CF-00-16-036 Date: January 24, 2017		
Rec. #		
1	<i>Finding</i>	<u>Campaign Receipts Applied to the Wrong Campaign Period</u> - The Principal Combined Fund Organization applied \$155,036 in 2014 campaign period receipts to the 2013 campaign period.
	<i>Recommendation</i>	We recommend the OCFO and the LFCC instruct the PCFO to disburse \$155,036 to the charities of the 2014 CFC.
	<i>Status</i>	This recommendation was closed after September 30, 2017.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	To ensure that donor wishes are honored and that federal employee donations go to the charities which are relying on these amounts to fulfill their organization's missions.
2	<i>Finding</i>	<u>Unclaimed Campaign Distributions Were Not Reissued</u> - The PCFO failed to reissue \$15,230 in 2013 campaign distributions that were either returned or uncashed.
	<i>Recommendation</i>	We recommend the OCFO and the LFCC instruct the PCFO to reissue \$15,230 in 2013 campaign distributions that were either returned or uncashed.
	<i>Status</i>	This recommendation was closed after September 30, 2017.
	<i>Estimated Program Savings</i>	\$15,230
	<i>Other Nonmonetary Benefit</i>	To ensure that donor wishes are honored and that federal employee donations go to the charities which are relying on these amounts to fulfill their organization's missions.

VII. EVALUATIONS

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

Title: Evaluation of OPM's Federal Worker's Compensation Program		
Report #: 4K-RS-00-15-050		
Date: March 29, 2016		
Rec. #		
1	Finding	Potential of Fraudulent Payments to Ineligible Beneficiaries - OPM's long-term FECA cases may be vulnerable to possible fraudulent payments.
	Recommendation	The OIG recommends that Employee Services work with the OIG's Office of Investigations to develop-a-process to refer any suspected FECA cases of fraud.
	Status	OPM agreed with this recommendation. The OIG has not yet received evidence that implementation has been completed.
	Estimated Program Savings	N/A
	Other Nonmonetary Benefit	The development of this process will reduce the risk of fraudulent FECA compensation payments being made to ineligible beneficiaries.

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

Continued: Evaluation of OPM's Retirement Services' Customer Service Function

Rec. #		
2	<i>Finding</i>	<u>Retirement Services is Not Providing Timely Responses to Annuitants' Inquiries</u> – The OIG found that Retirement Services is not meeting its goal to respond to all written correspondence.
	<i>Recommendation</i>	The OIG recommends Retirement Services allocate additional resources to address the backlog of written correspondences.
	<i>Status</i>	The agency agreed with this recommendation and is taking corrective action. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	By addressing the backlog of written correspondences, annuitants written inquires would be answered in a timely manner and customer satisfaction would improve.
3	<i>Finding</i>	<u>Annuitants Experience Difficulty Accessing RS's Customer Service:</u> We found that annuitants using the toll-free number are experiencing difficulty accessing RS's customer service. Specifically, annuitants are receiving excessive busy signals and long wait times when attempting to contact RS.
	<i>Recommendation</i>	The OIG recommends that RS develop a plan of action to reduce the specialists to customer ratio to increase the access to RS customer service via the toll-free number.
	<i>Status</i>	The agency agreed with this recommendation and is taking corrective action. The OIG has not yet received evidence that implementation has been completed.
	<i>Estimated Program Savings</i>	N/A
	<i>Other Nonmonetary Benefit</i>	We believe if the specialists to customer ratio is reduced, access to RS customer service via the toll-free number would increase, reducing busy signals and long wait times.

APPENDIX A

Below is a chart listing all reports described in this document which, as of September 30, 2017, had open recommendations over six months old.

Internal Operations Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4A-CF-00-08-025	FY 2008 Financial Statements	11/14/2008	6	1	0	\$0
4A-CF-00-09-037	FY 2009 Financial Statements	11/13/2009	5	1	0	\$0
4A-CF-00-10-015	FY 2010 Financial Statements	11/10/2010	7	3	0	\$0
1K-RS-00-11-068	Stopping Improper Payments to Deceased Ann.	09/14/2011	14	3	0	\$0
4A-CF-00-11-050	FY 2011 Financial Statements	11/14/2011	7	1	0	\$0
4A-CF-00-12-039	FY 2012 Financial Statements	11/15/2012	3	1	0	\$0
1K-RS-00-12-031	OPM's VOIP Interagency Agreement	12/12/2012	2	1	0	\$0
4A-CF-00-13-034	FY 2013 Financial Statements	12/13/2013	1	1	0	\$0
4A-CF-00-14-009	FY 2013 IPERA	04/10/2014	1	1	0	\$0
4A-CF-00-14-039	FY 2014 Financial Statements	11/10/2014	4	3	0	\$0
4K-RS-00-14-076	OPM's Compliance with FOIA	03/23/2015	3	2	0	\$0
4A-RS-00-13-033	Assessing Internal Controls over OPM's RES	04/13/2015	7	1	0	\$0
4A-CF-00-15-025	FY 2014 IPERA	05/15/2015	4	2	0	\$0
4A-HR-00-13-055	Human Resources Solutions' Pricing Method	06/02/2015	5	5	0	\$0
4A-CF-00-15-027	FY 2015 Financial Statements	11/13/2015	5	5	0	\$0
4K-RS-00-16-024	OPM's Credit Monitoring & Identity Theft	12/02/2015	2	2	0	\$0
4A-CF-00-16-026	FY 2015 IPERA	05/11/2016	6	5	0	\$0
4A-CA-00-15-041	OPM's OPO's Contract Management Process	07/08/2016	6	5	1	\$108,880,417
4A-CF-00-16-030	FY 2016 Financial Statements	11/14/2016	22	22	0	\$0
19	Total Reports		110	65	1	\$108,880,417

Information Systems Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4A-CI-00-08-022	FISMA FY 2008	09/23/2008	19	2	0	\$0
4A-CI-00-09-031	FISMA FY 2009	11/05/2009	30	2	0	\$0
4A-CI-00-10-019	FISMA FY 2010	11/10/2010	41	2	0	\$0
4A-CI-00-11-009	FISMA FY 2011	11/09/2011	29	3	0	\$0
4A-OP-00-12-013	IT Security Controls OPM's ARRTS	07/16/2012	24	5	0	\$0
4A-CI-00-12-016	FISMA FY 2012	11/05/2012	18	4	0	\$0
4A-CI-00-13-021	FISMA FY 2013	11/21/2013	16	5	0	\$0
4A-CI-00-14-015	IT Security Controls OPM's DTP	06/06/2014	6	5	0	\$0
4A-CI-00-14-016	FISMA FY 2014	11/12/2014	29	15	0	\$0
4A-CI-00-15-055	Flash Audit: OPM's Infrastructure Improvement	06/17/2015	2	1	0	\$0
4A-RI-00-15-019	IT Sec. Controls OPM's AHBOSS	07/29/2015	7	6	0	\$0
4A-HR-00-15-015	IT Sec. Controls OPM's GPB6 LMS	07/31/2015	12	2	0	\$0
4A-CI-00-15-011	FISMA FY 2015	11/10/2015	27	16	0	\$0
4A-CI-00-16-037	2nd Status Report::OPM's Infrastructure Improvement	05/18/2016	2	2	0	\$0
4A-CI-00-16-061	Web Application Security Review	10/13/2016	4	4	0	\$0
4A-CI-00-16-039	FISMA FY 2016	11/09/2016	26	22	0	\$0
4A-RS-00-16-035	IT Sec. Controls OPM's FACES	11/21/2016	13	11	0	\$0
17	Total Reports		305	107	0	\$0

Experience-Rated Insurance Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
1A-99-00-14-046	Global COB for BCBS Plans	07/29/2015	5	0	1	\$4,486,775
1A-10-17-14-037	Health Care Service Corporation	11/19/2015	16	2	1	\$34,896,254
1A-99-00-15-008	Global BCBS Claims-to-Enrollment Match	01/21/2016	8	3	2	\$6,078,939
1A-99-00-15-047	Global OBRA 90 for BCBS Plans	06/17/2016	5	2	1	\$1,411,302
1A-99-00-15-060	Global COB for BCBS Plans	10/13/2016	3	0	2	\$4,358,321
1A-10-33-15-009	BCBS of North Carolina	11/10/2016	6	2	4	\$18,151,063
6	Total Reports		43	9	11	\$69,382,654

Community-Rated Insurance Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
1C-QA-00-14-045	Independent Health	08/12/2015	3	0	2	\$9,558,728
1C-L4-00-16-013	HMO Health Ohio	09/23/2016	2	0	2	\$3,483,988
1C-JN-00-16-019	Aetna Open Access - Capitol Region*	01/31/2017	5	1	1	\$0
3	Total Reports		10	1	5	\$13,042,716

*All of the recommendations in this report were closed after September 30, 2017.

Other Benefit Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
1H-01-00-12-072	BCBS Retail Pharmacy Member Eligibility	11/08/2013	11	0	7	\$2,254,117
4A-RI-00-16-014	Mgmt Alert – OPM’s Procurement Process	10/14/2015	4	2	0	\$0
2	Total Reports		15	2	7	\$2,254,117

Combined Federal Campaign Audits						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
3A-CF-00-16-036	2013-2015 National Capital Area CFC*	01/24/2017	2	0	2	\$170,266
1	Total CFC Reports		2		2	\$170,266

**All of the recommendations in this report were closed after September 30, 2017.*

Evaluations						
Report Number	Name	Date	Total # of Findings	# of Open Procedural Findings	Monetary Findings	
					# Open	Amount
4K-RS-00-15-050	OPM's Federal Workers' Compensation	03/29/2016	5	1	0	0
4K-RS-00-16-023	OPM's Retirement Services' Customer Service	09/28/2016	3	3	0	0
2	Total Reports		8	4	0	0



Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: <http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse>

By Phone: Toll Free Number: (877) 499-7295
Washington Metro Area: (202) 606-2423

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100