



BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <b>1A-99-00-14-046</b>		Date Issued: <b>July 29, 2015</b>				
Subject: <b>Global COB for BCBS Plans</b>		Report Type: <b>FEHBP – BlueCross BlueShield Plans</b>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Global Coordination of Benefits Review</u> – Blue Cross Blue Shield (BCBS) plans incorrectly paid 9,028 claims, resulting in \$2,947,816 in overcharges to the Federal Employees Health Benefits Program (FEHBP). These claims should have been paid by Medicare, with only supplemental coverage provided by the FEHBP. However, the plans incorrectly billed the FEHBP as the primary insurer.	The OIG recommends that the OPM contracting officer disallow \$2,947,816 for claim overpayments and verify that the BCBS plans return all amounts recovered to the FEHBP.	Agreed: \$2,478,064  Disagreed: \$469,752	As of March 31, 2017: Collected: \$2,266,200 Receivable: \$211,864  <u>Estimated Time Frame For Implementation:</u> Long-term	Total Savings when Implemented: \$2,478,064 Sep 1, 2013 - May 31, 2014	N/A
5	<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.	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.	OPM is still reviewing this recommendation	<u>Estimated Time Frame For Implementation:</u> Long-term	Total Savings when Implemented: \$4,486,775 Sep 1, 2013 - May 31, 2014	N/A



BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <b>1A-10-17-14-037</b>		Date Issued: <b>November 19, 2015</b>				
Subject: <b>Health Care Service Corporation</b>		Report Type: <b>FEHBP – BlueCross BlueShield Plans</b>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Veterans Affairs (VA) Claim Review</u> HCSC incorrectly paid 13,108 VA claims, resulting in overcharges of \$35,562,962 to the FEHBP. For most of these claims, the Plan paid the full, undiscounted charges when lower payment rates could have been negotiated.	The OIG recommends that the contracting officer disallow \$35,562,962 for claim overcharges and verify that the Plan returns all amounts recovered to the FEHBP.	Agreed: \$35,560,326  Disagreed: \$2,636	As of March 31, 2017: Collected: \$548,335 Receivable: \$35,011,991 Contested: \$2,636  <u>Estimated Time Frame For Implementation:</u> Long-term	Total Savings when Implemented: \$35,560,326 Jan 1, 2012 - Dec 31, 2014	N/A
2	<u>Veterans Affairs Claim Review</u> HCSC incorrectly paid 13,108 VA claims, resulting in overcharges of \$35,562,962 to the FEHBP. For most of these claims, the Plan paid the full, undiscounted charges when lower payment rates could have been negotiated.	The OIG recommends that the OPM 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.	OPM is still reviewing this recommendation.	<u>Estimated Time Frame For Implementation:</u> Long-term	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.	Improved controls over ensuring VA claims are processed appropriately.



BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017

4	<p><u>Veterans Affairs Claim Review HCSC</u> incorrectly paid 13,108 VA claims, resulting in overcharges of \$35,562,962 to the FEHBP.</p> <p>These overcharges resulted in increased administrative expenses being charged to the FEHBP, because in some cases allocation rates are based on claims payments.</p>	<p>The OIG recommends that the OPM contracting officer request the Association to perform a risk assessment to determine the impact of the claim payment overcharges on administrative expenses charged to the FEHBP.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>Unknown: however, if implemented this should result in an increased savings from Jan 1, 2012 - Dec 31, 2014.</p>	<p>N/A</p>
16	<p><u>Non-Participating Provider Review:</u> The BCBS Association's guidance to BCBS Plans related to Indian Health Service (IHS) for payment to third party providers no longer reflects recent changes in federal regulations as described in the Indian Health Care Improvement Reauthorization and Extension Act.</p>	<p>The OIG recommends that the OPM contracting officer ensure the BCBS Association updates guidance to reflect the proper pricing for IHS. Additionally, the contracting officer should ensure that all BCBS Plans are properly notified of the changes for processing IHS claims.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Short-term</p>	<p>N/A</p>	<p>Improved controls over ensuring IHS claims are processed appropriately.</p>



BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <b>1A-99-00-15-008</b>		Date Issued: <b>January 21, 2016</b>				
Subject: <b>Global BCBS Claims-to-Enrollment Match</b>		Report Type: <b>FEHBP – BlueCross BlueShield Plans</b>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claims, 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 when medical services were rendered.	The OIG recommends that the OPM 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.	Agreed: \$8,229,632  Disagreed: \$1,821,377	As of March 31, 2017: Collected: \$5,311,665 Receivable: \$2,917,967 Uncollectible: \$1,472,021 Contested: \$349,356  <u>Estimated Time Frame For Implementation:</u> Long-term	Total Savings when Implemented: \$8,229,632 Jan 1, 2012 - Sept 30, 2014 (Recovered + Receivable)	N/A
2	<u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claims, resulting in overcharges of \$10,051,009 to the FEHBP.  Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.	Due to the number of errors related to retroactive enrollment adjustments, the OIG recommends that the BCBS Association promptly resolves enrollment discrepancies identified during the quarterly enrollment reconciliation process.	Agreed	OPM is taking action. The OIG has not received evidence that implementation has been completed.  <u>Estimated Time Frame For Implementation:</u> Long-term	Unknown – however, improved controls for updating enrollment records should result in increased program savings.	Improved controls over processing claims for only eligible members.



BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017

3	<p><u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claims, resulting in overcharges of \$10,051,009 to the FEHBP.</p> <p>Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.</p>	<p>The OIG recommends that the BCBS Association automate the process of updating the FEP Express claims processing system when enrollment discrepancies are identified.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>Unknown – however, improved system controls for updating enrollment records should result in increased program savings.</p>	<p>Improved controls over processing claims for only eligible members.</p>
4	<p><u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claims, resulting in overcharges of \$10,051,009 to the FEHBP.</p> <p>Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.</p>	<p>The OIG recommends that the BCBS Association 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).</p>	<p>OPM is still reviewing this recommendation</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>Unknown – however, improved controls for detecting fraud and abuse should result in increased program savings.</p>	<p>Improved controls for reporting fraud and/or abuse due to enrollment misrepresentation.</p>
5	<p><u>Global Claims-to-Enrollment Match Review</u> - BCBS plans incorrectly paid 45,473 claims, 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.</p> <p>Of these 45,473 claims, 40,077 claims were questioned due to retroactive enrollment adjustments.</p>	<p>The OIG recommends that the BCBS Association immediately update its “60-day recovery limit” policy that limits the BCBS plans from initiating recovery for at least 60 days on all retroactive enrollment terminations or cancellations.</p>	<p>OPM is still reviewing this recommendation</p>	<p><u>Estimated Time Frame For Implementation:</u> Short-term</p>	<p>Unknown – however, improved controls for initiating recoveries should result in increased program savings.</p>	<p>Improved controls for initiating recovery on claims paid for ineligible patients.</p>



BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017

6	<p><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.</p> <p>Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.</p>	<p>The OIG recommends that the OPM contracting officer require the Association to enhance the FEP Express system by adding an edit that defers claims when a patient's enrollment is incomplete or who has coverage under another FEP member number.</p>	<p>OPM is still reviewing this recommendation</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>Unknown – however, improved system controls should result in increased program savings.</p>	<p>Improved controls over processing claims for only eligible members.</p>
7	<p><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.</p> <p>Of these 45,473 claims, 40,077 were questioned due to retroactive enrollment adjustments.</p>	<p>The OIG recommends that the OPM contracting officer require the Association to evaluate its procedures for notifying members that their coverage has been terminated. The Association should attempt to identify the cause(s) that led to nine percent of the members we reviewed not receiving notification of coverage termination. Once a cause is identified, appropriate corrective action should be implemented.</p>	<p>Agreed</p>	<p>OPM is taking action. The OIG has not received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>Unknown – however, improved processes should result in increased program savings.</p>	<p>Improved process for notifying members when membership is terminated.</p>
8	<p><u>Statistical Review of Member Enrollment Issues</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 BCBS plans incorrectly paid \$3,207,289 in claims paid to ineligible members.</p>	<p>The OIG recommends that the OPM contracting officer disallow \$3,207,289 for claims that were not paid in good faith and unreasonably charged to the FEHBP.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>Total Savings if Implemented: \$3,207,289 Jan 1, 2012 - Sept 30, 2014</p>	<p>N/A</p>



BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <b>1A-99-00-15-047</b>		Date Issued: <b>June 17, 2016</b>				
Subject: <b>Global OBRA 90 for BCBS Plans</b>		Report Type: <b>FEHBP – BlueCross BlueShield Plans</b>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Global Omnibus Budget Reconciliation Act of 1990 (OBRA 90)</u> – The OIG’s review of high dollar claims that were subject to or potentially subject to special OBRA 90 pricing guidelines determined that the BCBS plans overpaid 686 of these claims by \$10,792,073.	The OIG recommends that the OPM contracting officer disallow \$10,792,073 for claim overpayments and verify that the BCBS plans return all amounts recovered to the FEHBP.	Agreed: \$9,683,969  Disagreed: \$1,108,104	As of March 31, 2017: Collected: \$8,272,667 Receivable: \$1,411,302 Uncollectible: \$499,753 Contested: \$608,351  <u>Estimated Time Frame For Implementation:</u> Short-term	Total Savings when Implemented: \$9,683,969 Jan 1, 2012 - April 30, 2015	N/A
3	<u>Global Omnibus Budget Reconciliation Act of 1990</u> – The OIG’s 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.	The OIG recommends that the OPM 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.	OPM is still reviewing this recommendation.	<u>Estimated Time Frame For Implementation:</u> Long-term	Unknown – however, improved processes should result in increased program savings.	Improved systematic process for accurately pricing OBRA 90 claims.



*BCBS Audit Recommendations Over 6 Months Old, as of March 31, 2017*

4	<p><u>Global Omnibus Budget Reconciliation Act of 1990</u> – The OIG’s review determined that 418 claims were priced with outdated Medicare effective rates, resulting in net overcharges of \$2,911,375 to the FEBHP.</p>	<p>The OIG recommends that the BCBS Association include CMS pricing updates in the FEP Express system at the time the updates are released.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>Unknown – however, improved processes should result in increased program savings.</p>	<p>Improved systematic process for accurately pricing OBRA 90 claims.</p>
---	--	---	--	--	--	---



**Report #:** 3A-CF-00-14-049 **Date Issued:** February 11, 2015  
**Subject:** Audit of the 2011 – 2012 CFC Campaigns Administered by the United Way of Long Island **Report Type:** Combined Federal Campaign

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Agreed-Upon Procedures Not in Compliance with the Audit Guide</u> – The Independent Public Accountant (IPA) utilized by the Local Federal Coordinating Committee (LFCC) to complete the Agreed-Upon Procedures (AUP) audit of the 2011 campaign did not perform its review in accordance with the requirements of the Audit Guide.	The OIG recommends that OPM’s Office of the Combined Federal Campaign (OCFC) and the LFCC ensures that the IPA fully understands the CFC and its related regulations so that it will complete the Audit Guide’s AUPs correctly and completely.	Agreed	OPM is taking action. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame For Implementation:</u> Long-term	N/A	Improve controls 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	<u>Agreed-Upon Procedures Not in Compliance with the Audit Guide</u> – The IPA utilized by the LFCC to complete the AUP audit of the 2011 campaign did not perform its review in accordance with the requirements of the Audit Guide.	The OIG recommends that the OCFC ensures that the LFCC and the United Way of Long Island (UWLI) meet with the IPA prior to and during the AUP engagement to discuss the Audit Guide steps, and encourage the IPA to ask questions of the OCFC if it is unsure of how to complete any of the required procedures.	Agreed	OPM is taking action. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame For Implementation:</u> Long-term	N/A	Improve controls to ensure that donor wishes are honored and Improve that federal employee donations go to the charities which are relying on these amounts to fulfill their organization’s missions.



CFC Audit Recommendations Over 6 Months Old, as of March 31, 2017

3	<p><u>Unallowable Expenses</u> – The UWLI incorrectly charged \$10,791 for unallowable expenses that were either unauthorized, unreasonable, or did not relate to the 2012 campaign.</p>	<p>The OIG recommends that the OCFC and the LFCC require the UWLI to distribute \$10,791 in unallowable expenses as undesignated funds to the charities participating in the 2012 campaign and charge the 2013 campaign \$438 for mileage expense related to the 2013 CFC.</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	\$10,791	<p>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.</p>
4	<p><u>Unallowable Expenses</u> – The UWLI incorrectly charged \$10,791 for unallowable expenses that were either unauthorized, unreasonable, or did not relate to the 2012 campaign.</p>	<p>The OIG recommends that the OCFC and the LFCC instruct the UWLI to stop charging food and beverages to the CFC in accordance with OPM’s Directive Prohibiting the Approval of Costs Incurred for Meals and Entertainment.</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Improve controls 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.</p>
5	<p><u>Unallowable Expenses</u> – The UWLI incorrectly charged \$10,791 for unallowable expenses that were either unauthorized, unreasonable, or did not relate to the 2012 campaign.</p>	<p>The OIG recommends that the OCFC and the LFCC ensure that the UWLI develops and implements policies and procedures to ensure that prizes and gifts are modest in nature and value in accordance with 5 CFR 950.602(b).</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Improve controls 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.</p>



CFC Audit Recommendations Over 6 Months Old, as of March 31, 2017

6	<p><u>Unallowable Expenses</u> – The UWLI incorrectly charged \$10,791 for unallowable expenses that were either unauthorized, unreasonable, or did not relate to the 2012 campaign.</p>	<p>The OIG recommends that the OCFC and the LFCC require the UWLI to develop and implement policies and procedures to ensure that only those expenses related to the CFC are charged to the campaign and that the UWLI properly matches expense to receipts for each campaign period.</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Improve controls 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.</p>
9	<p><u>Review and Authorization of Expense Reimbursement</u> – The LFCC did not review or authorize the UWLI’s reimbursement of actual campaign expenses.</p>	<p>The OIG recommends that the OCFC direct the LFCC to implement policies and procedures to document its review of the UWLI’s actual campaign expenses, which should be supported by itemized receipts and invoices, to ensure that the expenses are allowable and applicable to the campaign.</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Improve controls 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.</p>
10	<p><u>Review and Authorization of Expense Reimbursement</u> – The LFCC did not review or authorize the UWLI’s reimbursement of actual campaign expenses.</p>	<p>The OIG recommends that the OCFC direct the LFCC to implement policies and procedures to document its authorization and approval of the UWLI’s reimbursement of actual campaign expenses.</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Improve controls 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.</p>



CFC Audit Recommendations Over 6 Months Old, as of March 31, 2017

11	<p><u>CFC Receipts Applied to the Wrong Campaign</u> – The UWLI incorrectly applied \$23,144 in 2013 CFC receipts to the 2012 campaign and \$346 in 2012 CFC receipts to the 2011 campaign.</p>	<p>The OIG recommends that the OCFC direct the LFCC to ensure that the UWLI develops and implements policies and procedures to begin tracking CFC receipts by payroll office and to accurately account for end of the year payroll receipts.</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Improve controls 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.</p>
16	<p><u>LFCC Member Not a Federal Employee</u> – The OIG identified one LFCC member listed in both the 2012 CFC Charity List and the LFCC roster who was not an active Federal employee.</p>	<p>The OIG recommends that the OCFC develops and implements regulations and/or memoranda which stipulate that LFCC members be comprised of active Federal employees.</p>	OPM is still reviewing this recommendation.	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Improve controls 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.</p>
18	<p><u>Program Concern Related to LFCC Participation</u> – The OIG’s audit identified several concerns with the LFCC’s participation in CFC matters.</p>	<p>As a result of the identified concerns, the OIG (with support from the UWLI) recommends that the OCFC replace the LFCC with members who can be actively involved in the CFC. LFCC members do not need to be agency heads. Instead, those replacements (Federal employees) that the LFCC members currently send to attend the LFCC meetings could replace the current LFCC. This will allow accurate record keeping and voting related to CFC issues and LFCC meetings.</p>	Agreed	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	N/A	<p>Ensure that the campaign has the needed oversight so 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.</p>



CFC Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: 3A-CF-00-14-048 Date Issued: March 23, 2015  
 Subject: Audit of the 2011 – 2012 CFC Campaigns Administered by  
Community Shares of Minnesota Report Type: Combined Federal Campaign

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
15	<u>Undisbursed CFC Receipts</u> – CSM did not properly record all 2012 campaign receipts, which resulted in \$10,532 in campaign funds not being disbursed to charities.	The OIG recommends that the OCFC and the LFCC direct CSM to distribute \$10,532 in CFC funds to the charities that participated in the 2012 campaign.	Agreed	OPM is taking action. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame For Implementation:</u> Long-term	\$10,532	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.



**Report #:** 1C-QA-00-14-045 **Date Issued:** August 12, 2015  
**Subject:** Independent Health **Report Type:** FEHBP – Community-Rated HMO

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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>	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.	Partially agreed	<p>As of March 31, 2017:</p> <p>Receivable: \$8,828,534.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	Total Savings when Implemented: \$8,828,534	To ensure that Federal employees and their employing agencies are paying a fair and reasonable price for health coverage.
2	<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>	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.	<u>Agreed</u>	<p>As of March 31, 2017:</p> <p>Receivable: \$730,194 (lost investment income will continue to accrue until OPM is repaid)</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	Total Savings when Implemented: \$730,194 Total 1/1/12 – 7/31/2015 (plus interest since 8/1/2015)	To ensure that the Federal Government receives reimbursement for interest lost on Program funds due to improper payments.



**Report #:** 1C-22-00-14-071 **Date Issued:** August 31, 2015  
**Subject:** Aetna HealthFund **Report Type:** FEHBP – Community-Rated HMO

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><u>Medical Loss Ratio (MLR) Penalty Underpayment</u> – The Plan’s audited MLR of 83.25 percent was below OPM’s required threshold of 89 percent for contract year 2012. Factoring in a penalty payment of \$3,205,977 that the Plan had already remitted to OPM, the OIG determined that the Plan owed an additional penalty amount of \$20,016,333. Contributing to the additional penalty were the following factors:</p> <ul style="list-style-type: none"> <li>- A tax allocation method that was not applied proportionately, appropriately, and was not based on a generally accepted accounting method.</li> <li>- Dental claims that covered an incorrect time period.</li> <li>- Vendor payments that were inappropriately included as part of the incurred claims.</li> <li>- Pharmacy claims that were paid for ineligible members.</li> <li>- Incurred claims that were paid for non-covered benefits.</li> </ul>	<p>The OIG recommends that the OPM contracting officer require the Plan to return \$20,016,333 to the MLR subsidization penalty account for contract year 2012.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Short-term</p>	<p>Total Savings when <u>Implemented</u> \$20,016,333</p>	<p>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.</p>



HMO Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: **1C-51-00-14-066** Date Issued: **August 31, 2015**  
 Subject: **Health Insurance Plan of Greater New York** Report Type: **FEHBP – Community-Rated HMO**

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><u>Defective Pricing</u> - The Certificates of Accurate Pricing that Health Insurance Plan of Greater New York (Plan) signed for contract years 2013 and 2014 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 \$16,633,324.</p> <p>The OIG determined that defective pricing existed in 2013 and 2014 because the FEHBP's Medicare loading for each year was based on incomplete, inaccurate, and noncurrent Medicare enrollment data and applied incorrect copay level values.</p>	<p>The OIG recommends that the OPM contracting officer require the Plan to return \$16,633,324 to the FEHBP for defective pricing in contract years 2013 and 2014.</p>	Partially agreed	<p>As of March 31, 2017:</p> <p>Receivable: \$2,700,533.</p> <p><u>Est. Time Frame For Implementation</u>: Short-term.</p>	<p>Total Savings when Implemented: \$2,700,533</p>	<p>To ensure that Federal employees and their employing agencies are paying a fair and reasonable price for health coverage.</p>



*HMO Audit Recommendations Over 6 Months Old, as of March 31, 2017*

2	<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 2013 and 2014. We determined that the FEHBP is due \$557,854 for lost investment income, calculated through July 31, 2015.</p>	<p>The OIG recommends that the OPM contracting officer require the Plan to return \$557,854 to the FEHBP for lost investment income, calculated through July 31, 2015. We also recommend that the 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.</p>	Partially agreed	<p>As of March 31, 2017:  Receivable: \$136,764  <u>Est. Time Frame For Implementation</u>: Short-term.</p>	<p>Total Savings when Implemented: \$136,764  Total 1/1/13 – 7/31/2015  (plus interest since 8/1/2015)</p>	<p>To ensure that the Federal Government receives reimbursement for interest lost on Program funds due to improper payments.</p>
---	---	---	------------------	---	--	--



**Report #: 1C-2U-00-15-030** **Date Issued: May 10, 2016**  
**Subject: Aetna Open Access – Athens and Atlanta** **Report Type: FEHBP – Community-Rated HMO**

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><u>Medical Loss Ratio Penalty Underpayment</u> - The Plan's audited MLR of [REDACTED] percent was below OPM's required threshold of 85 percent for contract year 2013. This resulted in a subsidization penalty underpayment of \$766,267. Contributing to the penalty were the following factors:</p> <ul style="list-style-type: none"> <li>- A tax allocation method that was not applied proportionately, appropriately, and was not based on a generally accepted accounting method.</li> <li>- Medical and Pharmacy claims that were paid for ineligible members.</li> </ul>	<p>The OIG recommends that the OPM contracting officer require the Plan to return \$766,267 to the MLR subsidization penalty account for contract year 2013.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Est. Time Frame For Implementation:</u> Short-term.</p>	<p>Total Savings when Implemented:  \$766,267</p>	<p>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.</p>



**Report #:** 1C-HA-00-15-033 **Date Issued:** May 10, 2016  
**Subject:** Coventry Health Care of Kansas, Inc. **Report Type:** FEHBP – Community-Rated HMO

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><u>Medical Loss Ratio Penalty Underpayment</u> - The Plan's audited MLR of [REDACTED] percent was below OPM's required threshold of 85 percent for contract year 2013. This resulted in a subsidization penalty underpayment of \$121,675. Contributing to the penalty were the following factors:</p> <ul style="list-style-type: none"> <li>- A tax allocation method that was not applied proportionately, appropriately, and was not based on a generally accepted accounting method.</li> <li>- Incurred claims amount that was incorrect for pharmacy claims, capitations, dental claims, and pharmacy rebates.</li> <li>- Two medical claims that were incorrectly coordinated with Medicare.</li> </ul>	<p>The OIG recommends that the OPM contracting officer require the Plan to return \$121,675 to the MLR subsidization penalty account for contract year 2013.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Est. Time Frame For Implementation:</u> Short-term.</p>	<p>Total Savings when Implemented: \$121,675</p>	<p>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.</p>



**Report #:** 1C-JR-00-15-046 **Date Issued:** July 15, 2016  
**Subject:** Aetna Open Access – Northern New Jersey **Report Type:** FEHBP – Community-Rated HMO

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><u>Medical Loss Ratio Penalty Underpayment</u> – While the Plan’s audited MLR met the prescribed thresholds for 2012 and 2013, we identified the following concerns with portions of the MLR submissions that could impact future year’s MLR calculations if not corrected. These concerns include:</p> <ul style="list-style-type: none"> <li>- The Plan’s use of Direct Premiums Written to derive the large group premium ratio, which we believe does not produce the most accurate results.</li> <li>- A tax allocation method that was not applied proportionately, appropriately, and was not based on a generally accepted accounting method.</li> <li>- Medical and Pharmacy claims that were paid for ineligible members.</li> <li>- Medical claims that were paid for non-covered benefits.</li> </ul>	<p>The OIG recommends that the OPM contracting officer require the Plan to either calculate the FEHBP’s State and Federal income tax allocation using the premium ratio method or utilize a method which is well documented and supported.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Est. Time Frame For Implementation:</u> Short-term.</p>	<p>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.</p>	<p>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.</p>



**Report #: 1C-L4-00-16-013 Date Issued: September 23, 2016**  
**Subject: HMO Health Ohio Report Type: FEHBP – Community-Rated HMO**

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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>	<p>The OIG recommends that the OPM contracting officer either require the Plan to reimburse the FEHBP \$3,177,807 for defective pricing, or provide sufficient documentation to support the rate build-up for the [REDACTED]'s PPO product's rates in 2011 and 2012 so that the revenue neutrality resulting from the blending of the HMO and PPO rates can be validated.</p>	OPM is still reviewing this recommendation.	<u>Est. Time Frame For Implementation</u> : Short-term.	Total Savings when Implemented:  \$3,177,807	To ensure that Federal employees and their employing agencies are paying a fair and reasonable price for health coverage.
2	<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>	<p>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.</p>	OPM is still reviewing this recommendation.	<u>Est. Time Frame For Implementation</u> : Short-term.	Total Savings when Implemented:  \$306,181	To ensure that the Federal Government receives reimbursement for interest lost on Program funds due to improper payments.



Report #: <u>4A-CF-00-08-025</u>		Date Issued: <u>November 14, 2008</u>				
Subject: <u>Audit of the Fiscal Year 2008 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><u>Information Systems General Control Environment</u> – The Office of the Chief Information Officer (OCIO) has made progress in addressing information system general control deficiencies identified in previous years. However, some deficiencies have not been fully addressed. Specifically, 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.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	<p>The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.</p>



Report #: <u>4A-CF-00-09-037</u>		Date Issued: <u>November 13, 2009</u>				
Subject: <u>Audit of the Fiscal Year 2009 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4A-CF-00-10-015</u>		Date Issued: <u>November 10, 2010</u>				
Subject: <u>Audit of the Fiscal Year 2010 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	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	<u>Information Systems General Control Environment</u> – See number 1 above	KPMG recommends that the CIO identify common controls, control responsibilities, boundaries and interconnections for information systems in its system inventory.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



*Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017*

3	<u>Information Systems General Control Environment</u> – See number 1 above	KPMG recommends that the CIO implement a process to ensure the POA&Ms remains accurate and complete.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.
---	---	--	--------	---	-----	--



Report #: <u>1K-RS-00-11-068</u>		Date Issued: <u>September 14, 2011</u>				
Subject: <u>Stopping Improper Payments to Deceased Annuitants</u>		Report Type: <u>White Paper</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions. The OIG continues to have discussions with OPM about implementation.  <u>Est. Time Frame for Implementation:</u> Long-term	Potentially significant detection of and reduction in improper payments.	Updated annuity roll records.
2	<u>Capitalizing on RSM Technology</u> – A modernized environment offers opportunities to reduce instances of fraud, waste, and abuse of the retirement trust fund.	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.	Agreed	OPM is taking corrective actions. The OIG continues to have discussions with OPM about implementation.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	Improved detection of potential improper payments.



*Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017*

3	<p><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.</p>	<p>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.</p> <p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG continues to have discussions with OPM about implementation.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	Improved detection of potential improper payments.
---	---	--	--------	---	-----	--



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4A-CF-00-11-050</u>		Date Issued: <u>November 14, 2011</u>				
Subject: <u>Audit of the Fiscal Year 2011 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4A-CF-00-12-039</u>		Date Issued: <u>November 15, 2012</u>				
Subject: <u>Audit of the Fiscal Year 2012 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>1K-RS-00-12-031</u>		Date Issued: <u>December 12, 2012</u>				
Subject: <u>OPM's Voice over Internet Protocol Interagency Agreement</u>		Report Type: <u>Evaluation (Special Project)</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><u>Expense Documentation not Maintained</u> - After several attempts, OPM was unable to provide invoices documenting actual incurred contract expenses.</p> <p>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 only appropriate charges are being invoiced against OPM's contract.</p>	<p>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.</p>	<p>OPM's response does not address the finding and recommendation .</p>	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame for Implementation:</u> Long-term</p>	N/A	<p>Improved controls over the financial aspects of IAs when buying goods and services.</p>



Report #: <u>4A-CF-00-13-034</u>		Date Issued: <u>December 13, 2013</u>				
Subject: <u>OPM's Fiscal Year 2013 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4A-CF-00-14-009</u>		Date Issued: <u>April 10, 2014</u>				
Subject: <u>U.S. OPM's FY 2013 Improper Payments Reporting</u>		Report Type: <u>Internal Audit - Compliance</u>				
Rec #	Finding Title & Brief Description	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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.



Report #: <u>4A-CF-00-14-039</u>		Date Issued: <u>November 10, 2014</u>				
Subject: <u>OPM's Fiscal Year 2014 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding Title & Brief Description	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Information Systems Control Environment</u> - Significant deficiencies still remain in OPM's ability to identify, document, implement, and monitor information system controls.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	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	<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.	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."	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

3	<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"> <li>• Granted to new users without following the OPM access approval process and quarterly reviews to confirm access approval were not consistently performed.</li> <li>• Not revoked immediately upon user separation and quarterly reviews to confirm access removal were not consistently performed.</li> </ul>	<p>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:</p> <ul style="list-style-type: none"> <li>• Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process.</li> <li>• 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.</li> </ul>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame for Implementation:</u> Long-term</p>	N/A	<p>The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.</p>
---	---	---	--------	--	-----	---



<b>Report #:</b> <u>4A-RS-00-13-033</u>	<b>Date Issued:</b> <u>April 13, 2015</u>
<b>Subject:</b> <u>Assessing the Internal Controls over OPM's Retirement Services Retirement Eligibility and Services Office</u>	<b>Report Type:</b> <u>Internal Audit - Performance</u>

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Short-term	NA	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.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4A-CF-00-15-025</u>		Date Issued: <u>May 15, 2015</u>				
Subject: <u>U.S. OPM's FY 2014 Improper Payments Reporting</u>		Report Type: <u>Internal Audit - Compliance</u>				
Rec #	Finding	Recommendation	Status		Estimate d Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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)	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4A-HR-00-13-055</u>		Date Issued: <u>June 2, 2015</u>				
Subject: <u>Human Resources Solutions' Pricing Methodologies</u>		Report Type: <u>Internal Audit - Performance</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Short-term	N/A	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.
2	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Short-term		Documented guidance regarding the support for pricing determinations will decrease the likelihood of under- or over-charging customer agencies.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

3	<p><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.</p>	<p>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.</p>	<p>Agreed</p>	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Short-term</p>	<p>Documented guidance regarding the support for pricing determinations will decrease the likelihood of under- or over-charging customer agencies.</p>
4	<p><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.</p>	<p>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.</p>	<p>Agreed</p>	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Short-term</p>	<p>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.</p>



*Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017*

5	<p><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.</p>	<p>The OIG recommends that HRS strengthen their internal controls to ensure that projects are properly reviewed and approved to prevent projects created in error.</p>	<p>Agreed</p>	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Short-term</p>	<p>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.</p>
---	--	--	---------------	---	--



Report #: <u>4A-CF-00-15-027</u>		Date Issued: <u>November 13, 2015</u>				
Subject: <u>OPM's Fiscal Year 2015 Financial Statements</u>		Report Type: <u>Internal Audit – Financial Statement</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Information Systems Control Environment</u> - The current authoritative guidance regarding two-factor authentication has not been fully applied.	KPMG recommends that the OCIO fully implement the current authoritative guidance regarding two-factor authentication.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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	<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.	KPMG recommends that the OCIO document and map access rights in OPM systems to personnel roles and functions, following the principle of “least privilege”.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

3	<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"> <li>• Granted to new users without following the OPM access approval process and quarterly reviews to confirm access approval were not consistently performed.</li> <li>• Not revoked immediately upon user separation and quarterly reviews to confirm access removal were not consistently performed.</li> <li>• Granted to a privileged account without following the OPM access approval process.</li> </ul>	<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"> <li>• Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process; and</li> <li>• 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.</li> </ul>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	<p>The continued implementation of planned security enhancements will assist in enhancing agency-wide monitoring of critical IT resources to prevent and detect unauthorized use.</p>
4	<p>A formalized system component inventory of devices to be assessed as part of vulnerability or configuration management processes was not maintained.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

5	<p><u>Entity Level Controls Over Financial Management</u> - 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.</p>	<p>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.</p>	<p>Agreed</p>	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	<p>N/A</p>	<p>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.</p>
---	--	---	---------------	--	------------	---



Report #: 4K-RS-00-16-024 Date Issued: December 12, 2015  
 Subject: Special Review of the U.S. OPM's Award of a Credit Monitoring and Identity Theft Services Contract to Winvale Group LLC, and it's Subcontractor, CSIdentity Report Type: Special Review

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	<p>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.</p>



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

	<p>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>					
2	See number 1 above for description.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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.



<b>Report #:</b> <u>4A-CF-00-16-026</u>	<b>Date Issued:</b> <u>May 11, 2016</u>
<b>Subject:</b> <u>U.S. OPM's FY 2015 Improper Payments Reporting</u>	<b>Report Type:</b> <u>Internal Audit - Compliance</u>

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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.
3	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time Frame For Implementation:</u> Short-term	N/A	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.



*Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017*

4	<u>Risk Assessments</u> - See number 3 above	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)	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time Frame For Implementation:</u> Short-term	N/A	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	<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.	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)	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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.
6	<u>Improper Payments Information in the Agency Financial Report Was Inaccurately Reported</u> - See number 5 above	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.  <u>Est. Time For Implementation:</u> Long-term	N/A	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



Report #: <u>4A-CA-00-15-041</u>		Date Issued: <u>July 8, 2016</u>				
Subject: <u>U.S. OPM's Office of Procurement Operations' Contract Management Process</u>		Report Type: <u>Internal Audit – Performance</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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.
2	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Est. Time Frame For Implementation:</u> Long-term	N/A	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.



*Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017*

3	<p><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.</p>	<p>The OIG recommends that OPO develop an accurate inventory of FYs 2013 and 2014 contracts ready for closeout.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>		<p>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.</p>
4	<p><u>Weak Controls over the Contract Closeout Process</u> - See number 3 above</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	<p>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.</p>
5	<p><u>Weak Controls over the Contract Closeout Process</u> - See number 3 above</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	<p>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.</p>



*Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017*

6	<p><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.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p> <p><u>Est. Time Frame For Implementation:</u> Long-term</p>	N/A	<p>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.</p>
---	--	--	--------	--	-----	---



Internal Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4K-RS-00-14-076</u>		Date Issued: <u>March 23, 2015</u>				
Subject: <u>OPM's Compliance with the Freedom of Information Act</u>		Report Type: <u>Office of Audits Review</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	The OIG recommends that OPM's FOIA Office document a formal policy for handling multiple requests of the same information.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame for Implementation:</u> Long-term	N/A	Improved controls for managing FOIA information requests.
3	<u>Compliance with Electronic Freedom of Information Act Amendments of 1996</u> E-FOIA requires agencies to provide online reading rooms for citizens to access records and, in the instance of three or more requests for certain FOIA information that this information be posted in these rooms. OPM's website has a reading room that OPM's FOIA Office can use to post responses to multiple requests; however, we found that the reading room is not used.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame for Implementation:</u> Long-term	N/A	Improved controls for managing FOIA information requests.



<b>Report #:</b> <u>4A-CI-00-08-022</u>	<b>Date Issued:</b> <u>September 23, 2008</u>
<b>Subject:</b> <u>Federal Information Security Management Act Audit FY 2008</u>	<b>Report Type:</b> <u>Federal Information Security Management Act Audit</u>

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<p><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.</p> <p>However, we determined that the security controls were not tested for three of OPM’s systems in FY 2008.</p>	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.	Agreed	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
2	<p><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.</p> <p>We determined that the contingency plans for four OPM systems were not adequately tested in FY 2008.</p>	The OIG recommends that OPM’s program offices test the contingency plans for each system on an annual basis.	Agreed	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.	N/A	Improved controls for recovering from an unplanned system outage.



**Report #:** 4A-CI-00-09-031 **Date Issued:** November 5, 2009  
**Subject:** Federal Information Security Management Act Audit FY 2009 **Report Type:** Federal Information Security Management Act Audit

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
6	<u>Security Controls Testing</u> – FISMA requires agencies to test the security controls of all of their systems on an annual basis. In FY 2009, two systems did not have adequate security control tests.	The OIG recommends that 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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
9	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.	N/A	Improved controls for recovering from an unplanned system outage.



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

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
10	<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 2010, 15 systems did not have adequate security control tests.	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
30	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for recovering from an unplanned system outage.



Report #: <u>4A-CI-00-11-009</u>		Date Issued: <u>November 9, 2011</u>				
Subject: <u>Federal Information Security Management Act Audit FY 2011</u>		Report Type: <u>Federal Information Security Management Act Audit</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
6	<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.	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).	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for managing information security risks at OPM
7	<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 2011, 12 systems were not subject to adequate security control tests.	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
19	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for recovering from an unplanned system outage.





*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

15	<u>Identifier Management</u> - There is no process in place to routinely audit active user accounts to look for duplicate accounts.	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.	Agreed	Corrective actions are on hold because use of the system has been temporarily suspended. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for granting appropriate access to information systems.
17	<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.	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.	Agreed	Corrective actions are on hold because use of the system has been temporarily suspended. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for granting appropriate access to information systems.



**Report #:** 4A-CI-00-12-016 **Date Issued:** November 5, 2012  
**Subject:** Federal Information Security Management Act Audit FY 2012 **Report Type:** Federal Information Security Management Act Audit

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for managing information security risks at OPM.
11	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for authenticating to information systems.
14	<u>Test of Security Controls</u> - FISMA requires agencies to test the security controls all of their systems on an annual basis. In FY 2012, 13 systems were not subject to adequate security control tests.	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

15	<p><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.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.</p>	N/A	<p>Improved controls for recovering from an unplanned system outage.</p>
----	--	--	--------	---	-----	--



<b>Report #:</b> <u>4A-CI-00-13-021</u>		<b>Date Issued:</b> <u>November 21, 2013</u>	
<b>Subject:</b> <u>Federal Information Security Management Act Audit FY 2013</u>		<b>Report Type:</b> <u>Federal Information Security Management Act Audit</u>	

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring stability of systems development projects.
3	<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	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).	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for managing information security risks at OPM.
11	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for authenticating to information systems.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

13	<p><u>Test of Security Controls</u> - FISMA requires agencies to test the security controls of all their systems on an annual basis. In FY 2013, 13 systems were not subject to adequate security control tests.</p>	<p>The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.</p>	Agreed	<p>OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.</p>	N/A	<p>Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.</p>
14	<p><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 systems were not subject to adequate contingency plan tests.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.</p>	N/A	<p>Improved controls for recovering from an unplanned system outage.</p>





*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

5	<p><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.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for managing changes to information systems.</p>
6	<p><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.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for adequately segregating development, test, and production technical environments.</p>



Report #: <u>4A-CI-00-14-028</u>		Date Issued: <u>July 9, 2014</u>				
Subject: <u>Status of Cloud Computing within OPM</u>		Report Type: <u>Special Audit</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<u>FedRAMP Compliance</u> - no OPM cloud-based systems are currently using FedRAMP approved cloud service providers.	The OIG recommends that the OCIO update its cloud computing policies and procedures to incorporate FedRAMP requirements.	Agreed	This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring that cloud-based systems are supported by a FedRAMP compliant contractor.
3	<u>FedRAMP Compliance</u> - no OPM cloud-based systems are currently using FedRAMP approved cloud service providers.	The OIG recommends that the OCIO require all program offices with cloud-based systems to use CSPs that are FedRAMP compliant.	Partially Agreed	This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring that cloud-based systems are supported by a FedRAMP compliant contractor.





Report #: <u>4A-CI-00-14-016</u>		Date Issued: <u>November 12, 2014</u>				
Subject: <u>Federal Information Security Management Act Audit FY 2014</u>		Report Type: <u>Federal Information Security Management Act Audit</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring stability of systems development projects.
3	<u>Security Assessment and Authorization</u> – Eleven OPM systems are operating without an active Security Assessment and Authorization.	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.	Agreed	OPM is taking corrective actions. OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
4	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.



IT Audit Recommendations Over 6 Months Old, as of March 31, 2017

5	<p><u>Security Assessment and Authorization</u> – Several OPM systems are operating without an active Security Assessment and Authorization. These systems are not being subjected to routine security control evaluations, therefore are at increased risk of containing an unidentified security weakness that could lead to a data breach.</p>	<p>The OIG recommends that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.</p>
6	<p><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.</p>	<p>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).</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for managing information security risks at OPM.</p>
7	<p><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.</p>	<p>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 ██████████.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that information systems are initially configured in a secure manner.</p>
8	<p><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.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that servers are in compliance with approved security settings.</p>



IT Audit Recommendations Over 6 Months Old, as of March 31, 2017

11	<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.	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for detecting and vulnerabilities.
12	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for tracking and remediating vulnerabilities.
14	<u>Patching Management</u> - Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for keeping information systems up-to-date with patches and service packs.
21	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for authenticating to information systems.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

23	<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.	The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
24	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for recovering from an unplanned system outage.
25	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for recovering from an unplanned system outage.
28	<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.	The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

29	<p><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.</p>	<p>The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.</p>	<p>Agreed</p>	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	<p>N/A</p>	<p>Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.</p>
----	--	---	---------------	--	------------	--



Report #: <u>4A-CI-00-14-064</u>		Date Issued: <u>January 14, 2015</u>				
Subject: <u>Audit of Information Security Controls @ OPM's DMRS</u>		Report Type: <u>Federal Information Security Management Act Audit – OPM Computer System</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<u>Audit and Accountability</u> – The current version of ██████████ utilized by DMRS does not support any auditing capabilities.	The OIG recommends that FIS implement technical controls on DMRS to track system events in accordance with the NIST SP 800-53 Revision 4 Audit and Accountability control family.	Agreed	This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring that system events can be tracked and monitored.
3	<u>Audit and Accountability</u> – The current version of ██████████ utilized by DMRS does not support any auditing capabilities.	The OIG recommends that FIS review its auditing and accountability policies and procedures and incorporate the technical controls implemented as part of Recommendation 2.	Agreed	This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring that system events can be tracked and monitored.
4	<u>Penetration Testing</u> – FIS/NBIB does not currently conduct routine penetration testing for DMRS as required by NIST 800-53 Revision 4.	The OIG recommends that FIS implement policies and procedures to conduct routine penetration testing on DMRS.	Disagreed	OPM subsequently agreed to implement this recommendation.  This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring that information system vulnerabilities are detected and remediated.



<b>Report #:</b> <u>4A-CI-00-15-055</u>	<b>Date Issued:</b> <u>June 17, 2015</u>
<b>Subject:</b> <u>Flash Audit: OPM's Infrastructure Improvement</u>	<b>Report Type:</b> <u>OPM Major Project Oversight</u>

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Disagree	OPM subsequently agreed to implement this recommendation.  The OIG reviewed evidence submitted by OPM to support closure of the recommendation and provided comments explaining why this evidence was not sufficient to close the recommendation.	N/A	Improved controls for minimizing the risk of a major project failure.







*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

5	Protection of Information at Rest – [REDACTED]	The OIG recommends that RS ensure that GDIT [REDACTED]	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for preventing unauthorized disclosure of sensitive data in the event of a system compromise.
6	<u>Vulnerability Scanning – System Patching</u> – Our independent vulnerability scans indicated that critical patches and service packs are not always implemented in a timely manner.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for maintaining current and up-to-date system software.
7	<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.	The OIG recommends that RS ensure that GDIT utilize automated software tools to perform configuration compliance audits of the AHBOSS servers.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for identifying insecure configuration settings.



<b>Report #:</b> <u>4A-HR-00-15-015</u>		<b>Date Issued:</b> <u>July 31, 2015</u>			
<b>Subject:</b> <u>Audit of Information Security Controls @ OPM's GP Plateau Baseline 6 Learning Management System</u>		<b>Report Type:</b> <u>Federal Information Security Management Act Audit – OPM Computer System</u>			

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<u>Security Assessment Plan (SAP) and Report (SAR)</u> – The GPB6 LMS SAP failed to identify a variety of systems to be assessed in the SAR. The SAR testing did not cover all of the components of the system inventory.	The OIG recommends that Human Resources Solutions (HRS) update the GPB6 LMS Security Assessment Plan and Report to including all appliances and devices within the system boundary. Any additional weaknesses that are identified should be added to the system's POA&M.	Disagree	This recommendation was closed after March 31, 2017.	N/A	Improved controls for identifying and accepting security risks.
4	<u>Privacy Impact Assessment (PIA)</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.	The OIG recommends that HRS complete a current Privacy Impact Assessment for the GPB6 LMS.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for identifying privacy vulnerabilities existing on the information system.
6	<u>Updated POA&amp;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.	The OIG recommends that HRS update the GPB LMS POA&M to include a new scheduled completion date for all delayed items.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for maintaining and documenting POA&M's.



**Report #:** 1C-E3-00-15-020 **Date Issued:** August 28, 2015  
**Subject:** Audit of Information System General & Application Controls @ Kaiser Mid-Atlantic **Report Type:** Community-Rated Employee Organization Plan

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Authentication Standards</u> – We identified information systems that do not enforce [REDACTED] restrictions. Kaiser’s policy also does not require [REDACTED] on all their passwords.	The OIG recommends that Kaiser configure all of its information systems to enforce [REDACTED].	Agreed	The OIG reviewed evidence submitted by OPM to support closure of the recommendation and provided comments explaining why this evidence was not sufficient to close the recommendation.	N/A	Improved controls for securing logical access to information systems.
2	<u>Privileged User Authentication</u> Kaiser utilizes temporary privilege escalation methods or a second administrator account when elevated privileges are needed, however, [REDACTED] for privileged accounts would improve this process.	The OIG recommends that Kaiser implement [REDACTED] for privileged user access to all information systems.	Agreed	The OIG reviewed evidence submitted by OPM to support closure of the recommendation and provided comments explaining why this evidence was not sufficient to close the recommendation.	N/A	Improved controls for authenticating and identifying privileged user accounts.



**Report #:** 4A-CI-00-15-011 **Date Issued:** November 10, 2015  
**Subject:** Federal Information Security Management Act Audit FY 2015 **Report Type:** Federal Information Security Management Act Audit

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency's progress as part of the next annual audit.	N/A	Improved controls for ensuring stability of systems development projects.
3	<u>Security Assessment and Authorization</u> – Eleven OPM systems are operating without an active Security Assessment and Authorization.	The OIG recommends that all active systems in OPM's inventory have a complete and current Authorization.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.
4	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

5	<p><u>Security Assessment and Authorization</u> – Several OPM systems are operating without an active Security Assessment and Authorization. These systems are not being subjected to routine security control evaluations, therefore they are at an increased risk of containing an unidentified security weakness.</p>	<p>The OIG recommends that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.</p>
7	<p><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.</p>	<p>The OIG recommends that OPM ensure that an annual test of security controls has been completed for all systems.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that systems have appropriate security controls in place and functioning properly.</p>
8	<p><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.</p>	<p>The OIG recommends that the OCIO develop and implement a baseline configuration for all operating platforms in use by OPM including, but not limited to, [REDACTED], [REDACTED], and [REDACTED].</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that information systems are initially configured in a secure manner.</p>



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

9	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring that servers are in compliance with approved security settings.
10	<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.	The OIG recommends that the OCIO implement a process to ensure routine vulnerability scanning is conducted on all network devices documented within the inventory.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for detecting and remediating vulnerabilities.
11	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for tracking and remediating vulnerabilities.
13	<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.	The OIG recommends the OCIO implement a process to ensure that only supported software and operating platforms are utilized within the network environment.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for ensuring up-to-date software and operating platforms.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

14	<u>Patching Management</u> - Through our independent vulnerability scans on a sample of servers we determined that numerous servers are not timely patched.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for keeping information systems up-to-date with patches and service packs.
16	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for authenticating to information systems.
18	<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.	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).	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for managing information security risks at OPM.
24	<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.	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.	Agreed	OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.	N/A	Improved controls for recovering from an unplanned system outage.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

25	<p><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.</p>	<p>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.</p>	Agreed	<p>OPM is taking corrective actions and the OIG will assess the agency’s progress as part of the next annual audit.</p>	N/A	<p>Improved controls for recovering from an unplanned system outage.</p>
26	<p><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.</p>	<p>The OIG recommends that the OCIO ensure that all ISAs are valid and properly maintained.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that security agreements between contractor systems and agency systems are adequately tracked and maintained.</p>
27	<p><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.</p>	<p>The OIG recommends that the OCIO ensure that a valid MOU/A exists for every interconnection.</p>	Agreed	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>Improved controls for ensuring that interfaces between contractor systems and agency systems are adequately tracked and maintained.</p>



**Report #:** 1C-3A-00-15-012 **Date Issued:** January 21, 2016  
**Subject:** Audit of Information System General & Application Controls @ AultCare **Report Type:** Community-Rated Employee Organization Plan

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
7	[REDACTED] - AultCare has not implemented technical controls to prevent [REDACTED]	The OIG recommends AultCare implement technical controls to prevent [REDACTED]	Agreed	This recommendation was resolved after March 31, 2017.	N/A	Improved controls for ensuring that only authorized devices can connect to proprietary networks.
9	<u>Vulnerability Scanning</u> - The results of our vulnerability scans test work indicate that AultCare's vulnerability management program could be improved.	The OIG recommends that AultCare make the appropriate changes to its servers, workstations, and web applications to address the specific vulnerabilities identified in our vulnerability scans.	Agreed	This recommendation was resolved after March 31, 2017.	N/A	Improved controls for detecting and remediating vulnerabilities.



**Report #:** 1C-76-00-15-021 **Date Issued:** February 16, 2016  
**Subject:** Audit of Information System General & Application Controls @ Union Health Services **Report Type:** Community-Rated Employee Organization Plan

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
13	<u>Unsupported Software</u> - The results of our vulnerability scans indicated that UHS's production environment contains out-of-date and unsupported software and operating platforms.	The OIG recommends that UHS implement a process to ensure only current and supported versions of software applications are installed on the production servers. This should include a process for documenting known instances where unsupported software is required for business reasons.	Agreed	The OIG reviewed evidence submitted by OPM to support closure of the recommendation and provided comments explaining why this evidence was not sufficient to close the recommendation.	N/A	Improved controls for ensuring up-to-date software and operating platforms.
15	<u>Baseline Configuration</u> - UHS has not documented formal baseline configurations for its computer servers. A baseline configuration is a formally approved standard outlining how to securely configure a specific operating platform.	The OIG recommends that UHS document approved baseline configurations for all operating platforms and databases that it uses in its technical environment.	Agreed	The OIG reviewed evidence submitted by OPM to support closure of the recommendation and provided comments explaining why this evidence was not sufficient to close the recommendation.	N/A	Improved controls for ensuring that information systems are initially configured in a secure manner.
16	<u>Configuration Auditing</u> - UHS does not maintain approved baseline configurations, and therefore cannot effectively audit its system security settings (i.e., there are no approved settings to which to compare the actual settings).	The OIG recommends that UHS implement a process to routinely audit security configuration settings to ensure they are in compliance with the approved configuration baselines.	Agreed	The OIG reviewed evidence submitted by OPM to support closure of the recommendation and provided comments explaining why this evidence was not sufficient to close the recommendation.	N/A	Improved controls for ensuring that servers are in compliance with approved security settings.



*IT Audit Recommendations Over 6 Months Old, as of March 31, 2017*

21	<p><u>Data Center Environmental Controls</u> - The current data center that hosts UHS information systems is a dedicated room within the organization's primary office and medical clinic. The facility provides some environmental controls to protect the availability of systems such as air cooling and alternate power sources. However, the environmental controls could be improved with the implementation of a fire suppression system.</p>	<p>The OIG recommends that UHS improve the environmental controls at the current server room in its primary facility. At a minimum, there should be a fire suppression system to respond to an emergency within that area.</p>	Agreed	This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring adequate environmental protection in the data center.
----	--	--	--------	--	-----	--



**Report #:** 4A-CI-00-16-037 **Date Issued:** May 18, 2016  
**Subject:** Second Status Report: OPM's Infrastructure Improvement **Report Type:** OPM Major Project Oversight

Rec #	Finding Title & Brief Description	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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).	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for minimizing the risk of a major project failure.
2	<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.	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	N/A	Improved controls for minimizing the risk of a major project failure.



**Report #:** 1D-89-00-16-011      **Date Issued:** September 28, 2016  
**Subject:** Audit of Information System General & Application Controls @ Triple-S Salud      **Report Type:** FEHBP -Experience-Rated Employee Organization Plan

Rec #	Finding Title & Brief Description	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
8	<u>Security Configuration Settings</u> – Triple-S has not documented formal baseline configurations for its computer servers. A baseline configuration is a formally approved standard outlining how to securely configure a specific operating platform.	The OIG recommends that Triple-S Salud document approved security configurations for all operating platforms and databases deployed in its technical environment.	Agreed	This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring that information systems are initially configured in a secure manner.
9	<u>Configuration Auditing</u> – Triple-S does not maintain approved baseline configurations, and therefore cannot effectively audit its system security settings (i.e., there are no approved settings to which to compare the actual settings).	The OIG recommends that Triple-S Salud implement a process to routinely audit the configuration settings of servers and databases to ensure they are in compliance with the approved security configuration standards.	Agreed	This recommendation was closed after March 31, 2017.	N/A	Improved controls for ensuring that servers are in compliance with approved security settings.



Special Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>1H-01-00-12-072</u>			Date Issued: <u>November 8, 2013</u>			
Subject: <u>Audit of BCBS Retail Pharmacy Member Eligibility</u>			Report Type: <u>Pharmacy Benefit Manager</u>			
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Partially agreed	The OIG continues to have discussions with OPM concerning the areas of disagreement.  <u>Estimated Time Frame For Implementation:</u> Long-Term	\$677,312	Improved controls to verify eligible members and prevent improper payments to ineligible members.
2	<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.	The OIG recommends that the contracting officer direct the Plan to return \$681,496 to the FEHBP for the projected eligibility errors for 2011.	OPM is still reviewing this recommendation.	<u>Estimated Time Frame For Implementation:</u> Long-term	\$681,496	Improved controls to verify eligible members and prevent improper payments to ineligible members.



*Special Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017*

3	<p><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.</p>	<p>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.</p>	Partially agreed	<p>The OIG continues to have discussions with OPM concerning the areas of disagreement.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	\$386,4971	<p>Improved controls to verify eligible members and prevent improper payments to ineligible members.</p>
---	---	---	------------------	--	------------	--



Special Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017

4	<p><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.</p>	<p>The OIG recommends that the OPM contracting officer direct the Plan to return \$478,133 to the FEHBP for projected eligibility errors for 2011.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>\$478,133</p>	<p>Improved controls to verify eligible members and prevent improper payments to ineligible members.</p>
7	<p><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.</p>	<p>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.</p>	<p>Partially agreed</p>	<p>The OIG continues to have discussions with OPM concerning the areas of disagreement.</p> <p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>\$49,089</p>	<p>Improved controls to verify eligible members and prevent improper payments to ineligible members.</p>



Special Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017

8	<p><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.</p>	<p>The OIG recommends that the OPM contracting officer direct the Plan to return \$24,200 to the FEHBP for projected eligibility errors for 2011.</p>	<p>OPM is still reviewing this recommendation.</p>	<p><u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>\$24,200</p>	<p>Improved controls to verify eligible members and prevent improper payments to ineligible members.</p>
10	<p><u>Member Eligibility Problems Identified</u> – Because of a high error rate of potential member eligibility errors identified in a previous audit, the OIG selected a statistical sample of member eligibility claims for 2006, 2007, and 2011 to determine if claims were properly paid.</p>	<p>The OIG recommends that the contracting officer direct the Plan to institute internal controls and edits to the eligibility system that would reject or suspend a claim for which no eligibility exists at the time of the claim.</p>	<p>Agreed</p>	<p>OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.</p>	<p>N/A</p>	<p>Improved controls to verify eligible members and prevent improper payments to ineligible members.</p>
11	<p><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.</p>	<p>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).</p>	<p>Agreed</p>	<p>Final amount due for LII is contingent upon the final determination of the other findings in this audit report.  <u>Estimated Time Frame For Implementation:</u> Long-term</p>	<p>\$6,465</p>	<p>N/A</p>



Report #: <u>1H-04-00-15-053</u>		Date Issued: <u>October 14, 2015</u>				
Subject: <u>Management Alert – Serious Concerns Related to OPM’s Procurement Process for Benefit Programs</u>		Report Type: <u>Management Alert Memo</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
2	<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).	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame For Implementation:</u> Long-term	Indirect Savings - Unknown	Improved controls to ensure compliance with FAR and to enhance procurements integrity within OPM.
3	Consolidation of Procurement Functions.	The OIG recommends that OPM consider consolidating all contract administration functions under its Office of Procurement Operations and that these responsibilities no longer be delegated to the program offices.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame For Implementation:</u> Long-term	Indirect Savings - Unknown	Improved controls to ensure compliance with FAR and to enhance procurements integrity within OPM.



*Special Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017*

4	See #3 Above	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.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed. <u>Estimated Time Frame For Implementation:</u> Long-term	Indirect Savings - Unknown	Improved controls to ensure compliance with FAR and to enhance procurements integrity within OPM.
---	--------------	--	--------	--	----------------------------	---



Report #: <u>1H-01-00-12-072</u>			Date Issued: <u>September 28, 2016</u>			
Subject: <u>Audit of APWU Health Plan's Pharmacy Operations</u>			Report Type: <u>Pharmacy Benefits Manager</u>			
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	The PBM was unable to accurately support all of the line items it charged to the Plan for administration of the pharmacy benefits. Specifically, administrative costs associated on a per-member per-month basis were not supported with accurate enrollment counts.	The OIG recommends that the OPM contracting officer and the Plan require the PBM to maintain complete and accurate documentation to support administrative fees and invoices billed (both the fees charged and quantities).	Agreed	This recommendation was closed after March 31, 2017.	Indirect Savings - Unknown	Improved controls to ensure compliance with FAR 31.2 and to enhance procurement integrity within OPM.
2	See #2 Above.	The OIG recommends that the OPM contracting officer require the Plan to implement policies and procedures for reviewing the administrative fees, including the verification of invoices to supporting documentation to ensure that invoices related to the FEHBP are paid accurately and in accordance with the Agreement.	Agreed	This recommendation was closed after March 31, 2017.	Indirect Savings - Unknown	Improved controls to ensure compliance with FAR 31.2 and to enhance procurement integrity within OPM.
3	The PBM paid claims dispensed to one pharmacy chain incorrectly for over six months due to an incorrect discount in its claims system.	The OIG recommends that the OPM contracting officer direct the Plan to reimburse \$5,064 to the FEHBP and \$4,890 to the affected Plan members.	Agreed	This recommendation was closed after March 31, 2017.	\$5,064 + unknown future savings	Improved controls to ensure compliance with the contract and to enhance procurement integrity within OPM.



Special Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017

6	The Plan paid 124 pharmacy claims, for 16 dependent children, that were ineligible for coverage due to being age 26 (or older) on the dates of service. As a result, the FEHBP was overcharged \$16,847.	The OIG recommends that the OPM contracting officer direct the Plan to return \$16,847 to the FEHBP for erroneous claim payments on ineligible coverage dependents.	Partially agreed	This recommendation was closed after March 31, 2017.	\$180 + Unknown Future Savings	Improved controls to verify eligible members and prevent improper payments to ineligible members.
9	Override codes were incorrectly applied by either the PBM or the Plan, resulting in 96 claim payment errors for contract years 2012 through 2014. Although the overpayments identified were immaterial, if the underlying cause is not corrected, significant overpayments may occur in the future.	The OIG recommends that the OPM contracting officer direct the Plan to ensure that all overrides, especially effecting coinsurance, are entered and applied correctly so that claims are paid correctly. Additionally, the Plan should institute procedures to review the initial paid claims with overrides to ensure that the coinsurance is paid correctly.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.	Indirect Savings - Unknown	Improved controls to ensure compliance with the contract and to enhance procurement integrity within OPM.
10	See #9 Above.	The OIG recommends that the OPM contracting officer direct the Plan to obtain from the PBM a list of all claim overrides in place and to review those overrides to ensure that they are still necessary. This should be done on an annual basis.	Agreed	OPM is taking corrective actions. The OIG has not yet received evidence that implementation has been completed.  <u>Estimated Time Frame For Implementation:</u> Short-term	Indirect Savings - Unknown	Improved controls to ensure compliance with the contract and to enhance procurement integrity within OPM.



*Special Audits Group Audit Recommendations Over 6 Months Old, as of March 31, 2017*

11	The Plan did not report to the OIG all of the suspected fraud and abuse cases that were received from the PBM.	The OIG recommends that the OPM contracting office ensure that the Plan has updated its policies and procedures so that all potential cases of fraud, waste, and abuse reported to the Plan by the PBM are referred to the OPM's OIG, in compliance with the most recent FEHBP Carrier Letter (CL 2014-29).	Agreed	This recommendation was closed after March 31, 2017.	Indirect Savings - Unknown	Improved controls to ensure compliance with the contract and CL 2014-29. Enhances procurement integrity within OPM.
13	The PBM did not submit the required 2014 annual performance report to the Plan by the due date in the Agreement. Furthermore, the PBM did not timely credit the Plan \$120,000 related to a performance standard that it failed to meet in CY 2014. Additionally, the Plan was not aware that the report was not submitted and a penalty was due until after the OIG identified the oversight in our audit.	The OIG recommends that the OPM contracting officer require the Plan and the PBM to develop policies and procedures to ensure that the annual performance report and any associated penalties are submitted to the Plan within the required deadlines.	Agreed	This recommendation was closed after March 31, 2017.	\$120,000 + unknown future savings	Improved controls to ensure compliance with the contract and to enhance procurement integrity within OPM.



Evaluation Recommendations Over 6 Months Old, as of March 31, 2017

Report #: <u>4K-RS-00-15-050</u>		Date Issued: <u>March 29, 2016</u>				
Subject: <u>OPM's Federal Worker's Compensation Program</u>		Report Type: <u>Office of Evaluations and Inspections</u>				
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<u>Potential of Fraudulent Payments to Ineligible Beneficiaries</u> - OPM's long-term FECA cases may be vulnerable to possible fraudulent payments.	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.	Agreed	As of March 31, 2017, Employee Services is waiting to receive additional information from the OIG's Office of Investigations.  <u>Est. Time Frame for Implementation:</u> Long-term	N/A	We believe the development of this process will reduce the risk of fraudulent FECA compensation payments being made to ineligible beneficiaries.



Report #: <u>4K-RS-00-16-023</u> Date Issued: <u>September 28, 2016</u>						
Subject: <u>Evaluation of OPM's Retirement Services' Customer Service Function</u> Report Type: <u>Office of Evaluations and Inspections</u>						
Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
1	<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.	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.	Partially Agreed	OPM is taking action. The OIG has not yet received evidence that implementation has been completed.	N/A	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.
2	<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.	The OIG recommends Retirement Services allocate additional resources to address the backlog of written correspondences.	Agreed	OPM is taking action. The OIG has not yet received evidence that implementation has been completed.	N/A	By addressing the backlog of written correspondences, annuitants written inquires would be answered in a timely manner and customer satisfaction would improve.



Report #: 4K-RS-00-16-023 Date Issued: September 28, 2016  
 Subject: Evaluation of OPM's Retirement Services' Customer Service Function Report Type: Office of Evaluations and Inspections

Rec #	Finding	Recommendation	Status		Estimated Program Savings	Other Non-monetary Benefit
			Agency Determination	Explanation		
3	<p><u>Annuitants Experience Difficulty Accessing RS's Customer Service</u></p> <p>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.</p>	<p>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.</p>	Agree	<p>OPM is taking action. The OIG has not yet received evidence that implementation has been completed.</p>	N/A	<p>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.</p>