



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Office of the Inspector General



SEMIANNUAL REPORT TO
CONGRESS

April 1, 2013 through September 30, 2013



Office of the Inspector General



Productivity Indicators

FINANCIAL IMPACT:

Audit Recommendations for Recovery of Funds	\$16,019,712
Management Commitments to Recover Funds	\$16,982,472
Recoveries Through Investigative Actions	\$31,184,915

Note: OPM management commitments for recovery of funds during this reporting period reflect amounts covering current and past reporting period audit recommendations.

ACCOMPLISHMENTS:

Audit Reports Issued	31
Evaluation Reports Issued	0
Investigative Cases Closed	28
Indictments and Informations	28
Arrests	18
Convictions	22
Hotline Contacts and Preliminary Inquiries Complaints	1,300
Health Care Provider Debarments and Suspensions	418
Health Care Provider Debarment and Suspension Inquiries	3,967

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Office of the Inspector General



SEMIANNUAL REPORT TO
CONGRESS

April 1, 2013 through September 30, 2013



INSPECTOR GENERAL'S MESSAGE

Traditionally, Inspectors General use this space to write a message to Congress about their offices' activities during the reporting period. This time, however, I would like to write about Congress, to tell the American taxpayers the story of how so many Members of Congress from diverse backgrounds have come together in the pursuit of good Government.

In the past, I have written about the near-debilitating limitations on our office's ability to provide adequate oversight of the \$2 billion Revolving Fund that finances certain programs operated by the U.S. Office of Personnel Management (OPM). One such program is the Federal Investigative Services, which conducts approximately 95 percent of the Federal Government's background investigations.

Based upon referrals of alleged fraud and identified audit risk factors, there is an urgent need for an immediate, strong, and continuing infusion of oversight of all Revolving Fund programs. Under the current funding structure, we are able to investigate only some of the most egregious allegations involving the programs and to conduct (at most) only one or two audits each year of Revolving Fund operations.

Over the past several years, we have met repeatedly with the Office of Management and Budget to discuss our concerns. In April 2013, the President included a proposal in his Fiscal Year 2014 Budget that would allow our office statutory access to the Revolving Fund to finance the level of oversight that these programs require. Shortly afterward, both the Senate Committee on Homeland Security and Government Affairs and the House Committee on Oversight and Government Reform took aggressive action to investigate and immediately address the problem. Staff from both Committees met with us several times in order to fully understand our dilemma so that they could take steps to rectify the situation. Both Committees then held hearings on the matter in June 2013. The very next month, Senator Jon Tester, Chairman of the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce, introduced S.1276, the Security Clearance Oversight and Reform Enhancement (SCORE) Act, on behalf of Senators Rob Portman, Claire McCaskill, Ron Johnson, and Tom Coburn. Shortly after, also in July, Congressman Blake Farenthold, Chairman of the Subcommittee on the Federal Workforce, U.S. Postal Service and the Census, introduced a similar bill, H.R. 2860, the OPM IG Act, on behalf of Congressman Stephen Lynch.

Through an admirable demonstration of bipartisan and bicameral cooperation, the champions of both bills have aggressively moved the bills forward. The SCORE Act was passed by the Senate on October 10, 2013, by unanimous consent. The OPM IG Act was marked-up and voted out of the House Committee on October 29, 2013.



INSPECTOR GENERAL'S MESSAGE

April 1, 2013 – September 30, 2013

Our Senate and House authorizing Committees have not been alone in taking action. The staff of the Senate and House Appropriations Committees also met with our office to learn more about the crisis we are facing. The Committees then included in their Appropriations Bills provisions addressing the lack of adequate funding for oversight of the Revolving Fund.

In a time when many citizens have become cynical about the workings of Government, this collaboration is a shining example of how, when faced with an unacceptable state of affairs, our leaders in both the Executive and Legislative Branches are working together to develop – and hopefully implement – a solution to ensure that taxpayer dollars are protected and the Government operates in the most efficient manner.

On behalf of my office, I offer my thanks to the Administration and Members of Congress for their leadership and support. I look forward to further proving that their belief in our work is deserving of the extraordinary efforts they have made.

A handwritten signature in black ink, reading "Patrick E. McFarland". The signature is fluid and cursive, with a large, sweeping flourish at the end.

Patrick E. McFarland
Inspector General



MISSION STATEMENT

Our mission is to provide independent and objective oversight of OPM services and programs.

We accomplish our mission by:

- Conducting and supervising audits, evaluations and investigations relating to the programs and operations of the U.S. Office of Personnel Management (OPM).
- Making recommendations that safeguard the integrity, efficiency and effectiveness of OPM services.
- Enforcing laws and regulations that protect the program assets that are administered by OPM.

Guiding Principles

We are committed to:

- Promoting improvements in OPM's management and program operations.
- Protecting the investments of the American taxpayers, Federal employees and annuitants from waste, fraud and mismanagement.
- Being accountable to the concerns and expectations of our stakeholders.
- Observing the highest standards of quality and integrity in our operations.

Strategic Objectives

The Office of the Inspector General will:

- Combat fraud, waste and abuse in programs administered by OPM.
- Ensure that OPM is following best business practices by operating in an effective and efficient manner.
- Determine whether OPM complies with applicable Federal regulations, policies, and laws.
- Ensure that insurance carriers and other service providers for OPM program areas are compliant with contracts, laws, and regulations.
- Aggressively pursue the prosecution of illegal violations affecting OPM programs.
- Identify, through proactive initiatives, areas of concern that could strengthen the operations and programs administered by OPM.



TABLE OF CONTENTS

PRODUCTIVITY INDICATORS	Inside Cover
INSPECTOR GENERAL'S MESSAGE	i
MISSION STATEMENTiii
FIELD OFFICES	vii
AUDIT ACTIVITIES	1
Health Insurance Carrier Audits	1
Information Systems Audits	6
Internal Audits	11
Special Audits	13
ENFORCEMENT ACTIVITIES	15
Investigative Cases	15
Administrative Sanctions of FEHBP Health Care Providers	23
STATISTICAL SUMMARY OF ENFORCEMENT ACTIVITIES	27
APPENDIX I - A: Final Reports Issued With Questioned Costs for Insurance Programs	29
APPENDIX I - B: Final Reports Issued With Recommendations for All Other Audit Entities	30
APPENDIX II: Final Reports Issued With Recommendations for Better Use of Funds	30
APPENDIX III: Insurance Audit Reports Issued	31
APPENDIX IV: Internal Audit Reports Issued	33
APPENDIX V: Information Systems Audit Reports Issued	33
APPENDIX VI: Summary of Audit Reports More Than Six Months Old Pending Corrective Action	34
APPENDIX VII: Most Recent Peer Review Results	37
APPENDIX VIII: Investigative Recoveries	38
INDEX OF REPORTING REQUIREMENTS	41



FIELD OFFICES





AUDIT ACTIVITIES

Health Insurance Carrier Audits

The United States Office of Personnel Management (OPM) contracts with private sector firms to provide health insurance through the Federal Employees Health Benefits Program (FEHBP). Our office is responsible for auditing the activities of this program to ensure that the insurance carriers meet their contractual obligations with OPM.

The Office of the Inspector General's (OIG) insurance audit universe contains approximately 230 audit sites, consisting of health insurance carriers, sponsors, and underwriting organizations. The number of audit sites is subject to yearly fluctuations due to the addition of new carriers, non-renewal of existing carriers, or health insurance plan mergers and acquisitions. The premium payments for the health insurance program are over \$45 billion annually.

The health insurance plans that our office audits are either community-rated or experience-rated carriers.

Community-rated carriers are comprehensive medical plans, commonly referred to as health maintenance organizations (HMOs).

Experience-rated carriers are mostly fee-for-service plans, the largest being the BlueCross and BlueShield health plans, but also include experience-rated HMOs.

The two types of carriers differ in the way they calculate premium rates. Community-rated carriers generally set their rates based on the average revenue needed to provide health benefits to each member of a group. Rates established by experience-rated plans reflect a given group's projected paid claims, administrative expenses, and service charges for administering a specific contract.

During the current reporting period, we issued 25 final audit reports on organizations participating in the FEHBP, of which 12 contain recommendations for monetary adjustments in the amount of \$16 million due the OPM administered trust funds.

COMMUNITY-RATED PLANS

The community-rated HMO audit universe covers approximately 120 health plans located throughout the country. Community-rated audits are designed to ensure that the premium rates plans charge the FEHBP are in accordance with their respective contracts and applicable Federal laws and regulations.

Federal regulations require that the FEHBP rates be equivalent to the rates a plan charges the two employer groups closest in subscriber size, commonly referred to as *similarly sized subscriber groups (SSSGs)*. The rates are set by the plan, which is also responsible for selecting the SSSGs. When an audit shows that the rates are not equivalent, the FEHBP is entitled to a downward rate adjustment to compensate for any overcharges.



AUDIT ACTIVITIES

April 1, 2013 – September 30, 2013

Community-rated audits focus on ensuring that:

- The plans select the appropriate SSSGs;
- The FEHBP rates are equivalent to those charged the SSSGs; and,
- The loadings applied to the FEHBP rates are appropriate and reasonable.

Loading is a rate adjustment that the FEHBP makes to the basic benefit package offered by a community-rated plan. For example, the FEHBP provides coverage for Federal annuitants. Many Federal annuitants may also be enrolled in Medicare. Therefore, the FEHBP rates may be adjusted to account for the coordination of benefits with Medicare.

During this reporting period, we issued 20 final audit reports on community-rated plans. These reports contain recommendations that require the health plans to return over \$7.4 million to the FEHBP. Summaries of two reports are provided below to highlight notable audit findings.

MVP Health Care – Central Region

SCHENECTADY, NEW YORK
Report No. 1C-M9-00-12-056
APRIL 1, 2013

MVP Health Care – Central Region (Plan) provides comprehensive medical services to its FEHBP members in the Central New York area. This audit covered contract years 2007 through 2010, and 2012. During this period, the FEHBP paid the Plan approximately \$229 million in premiums.

We identified \$2,291,168 in inappropriate health benefit charges to the FEHBP in 2007, 2008, and 2012. In addition, we determined the FEHBP is due \$432,665 for lost investment income as a result of the overcharges.

Lost investment income (LII) represents the potential interest earned on the amount the plan overcharged the FEHBP as a result of defective pricing.

The overcharges occurred because the Plan did not apply the largest SSSG discounts to the FEHBP rates in contract years 2007, 2008, and 2012. In addition, the Plan did not fully credit the FEHBP rates in contract year 2007 for a graduate medical expense/bad debt and charity surcharge that was included in the community rates. The graduate medical expense/bad debt and charity surcharge is an annual tax that New York health plans are charged for every non-FEHBP member enrolled in the state. Monies are pooled to fund state-operated programs used to cover both the medical expenses of state graduate students as well as the costs associated with medical bad debts and charity cases.

Furthermore, the Plan inappropriately charged the FEHBP in contract year 2012 for the health dollars benefit

loading program. A health dollars benefit loading is a non-FEHBP payment available to plan members to provide up to \$50 to spend during the year on health, wellness, and fitness programs.

Finally, the Plan did not comply with the record retention clause of its FEHBP contract. The Plan agreed with our findings and the full amount questioned was recovered.

Inappropriate Charges Amount to Over \$2 Million

Coventry Health Care of Kansas, Inc.

KANSAS CITY, MISSOURI
Report No. 1C-HA-00-12-069
JUNE 3, 2013

Coventry Health Care of Kansas, Inc. (Plan) provides comprehensive medical services to its FEHBP members throughout the Kansas City Metropolitan area (Kansas and Missouri) and the Wichita, Salina, and Central Kansas areas. This audit covered contract years 2009 and 2010. During this period, the FEHBP paid the Plan approximately \$93 million in premiums.



**Inappropriate
Charges
Amount to
\$115,153**

We identified \$115,153 in inappropriate health benefit charges to the FEHBP in contract year 2009. This overcharge occurred because the Plan did not correctly

calculate the benefit adjustment factors used to develop the FEHBP rates.

EXPERIENCE-RATED PLANS

The FEHBP offers a variety of experience-rated plans, including a service benefit plan and health plans operated or sponsored by Federal employee organizations, associations, or unions. In addition, experience-rated HMOs fall into this category. The universe of experience-rated plans currently consists of approximately 100 audit sites. When auditing these plans, our auditors generally focus on three key areas:

- Appropriateness of FEHBP contract charges and the recovery of applicable credits, including refunds;
- Effectiveness of carriers' claims processing, financial and cost accounting systems; and,
- Adequacy of carriers' internal controls to ensure proper contract charges and benefit payments.

During this reporting period, we issued four experience-rated final audit reports. In these reports, our auditors recommended that the plans return \$8.3 million in inappropriate charges and lost investment income to the FEHBP.

BlueCross BlueShield Service Benefit Plan

The BlueCross BlueShield Association (Association), on behalf of participating BlueCross BlueShield (BCBS) plans, entered into a Government-wide Service Benefit Plan with OPM to provide a health benefit plan authorized by the FEHB Act. The Association delegates authority to participating local BCBS plans throughout the United States to process the health benefit claims of its Federal subscribers.

The Association has established a Federal Employee Program (FEP) Director's Office, in Washington, D.C., to provide centralized management for the Service Benefit Plan. The FEP Director's Office coordinates the administration of the contract with the Association, BCBS plans, and OPM. The Association has also established an FEP Operations Center. The activities of the FEP Operations Center are performed by CareFirst BlueCross BlueShield, located in Washington, D.C. These activities include acting as fiscal intermediary between the Association and member plans, verifying subscriber eligibility, approving or disapproving the reimbursement of local plan payments of FEHBP claims, maintaining a history file of all FEHBP claims, and maintaining an accounting of all program funds.

The Association, which administers a fee-for-service plan known as the Service Benefit Plan, contracts with OPM on behalf of its member plans throughout the United States. The participating plans independently underwrite and process the health benefits claims of their respective Federal subscribers and report their activities to the national BCBS operations center in Washington, D.C. Approximately 62 percent of all FEHBP subscribers are enrolled in BCBS plans.

We issued three BCBS experience-rated reports during the reporting period. Experience-rated audits normally address health benefit payments, miscellaneous payments and credits, administrative expenses, and/or cash management activities. Our auditors identified \$8.3 million in questionable costs charged to the FEHBP contract. BCBS agreed with \$4.1 million of the identified overcharges. Summaries of two final reports are provided below to highlight our notable audit findings.

Global Audit of Continuous Stay Claims for BlueCross and BlueShield Plans

WASHINGTON, D.C.

Report No. 1A-99-00-13-004

AUGUST 20, 2013

We performed a limited scope performance audit to determine whether the BCBS plans complied with contract provisions relative to continuous stay claim payments.



AUDIT ACTIVITIES

April 1, 2013 – September 30, 2013

Continuous stay claims are two or more inpatient facility claims with consecutive dates of service that were billed by a provider for a patient with one length of stay.

Using our SAS data warehouse function, we performed a computer search on the BCBS claims database to identify continuous stay claims that were paid from January 2010 through July 2012. Based on this computer search, we identified 57,140 continuous stay claim groups (representing 126,476 claims), totaling approximately \$1.3 billion in payments. From this universe, we selected and reviewed a judgmental sample of 8,054 groups (representing 21,446 claims), totaling \$945,117,644 in payments. Our sample included all groups with cumulative claim payment amounts of \$35,000 or more for 59 of the 64 BCBS plans.

We determined that the BCBS plans incorrectly paid 659 continuous stay claims (630 from our sample and an additional 29 from an expanded review), resulting in net overcharges of \$6,259,347 to the FEHBP. Specifically, the BCBS plans overpaid 512 claims by \$9,713,652 and underpaid 147 claims

by \$3,454,305. Most of these claim payment errors were due to manual processing errors by BCBS plans and/or billing errors by providers.

The Association and/or BCBS plans agreed with \$3,436,554 of these questioned net overcharges.

**FEHBP
Overcharged
\$6.3 Million (net)
for Claim
Payment Errors**

reviewed Florida Blue’s Fraud and Abuse Program for the period 2010 through February 2012. For contract years 2009 through 2011, Florida Blue processed approximately \$3.6 billion in FEHBP health benefit payments and charged the FEHBP \$168 million in administrative expenses.

**Auditors
Question Over
\$1.7 Million in
Overcharges**

Our auditors questioned \$1,768,338 in health benefit charges and administrative expense overcharges; and identified a procedural finding regarding Florida Blue’s Fraud and Abuse Program. The monetary findings included the following:

- \$1,623,435 for plan employee post-retirement benefit cost overcharges;
- \$74,116 for administrative expense charges that were unallowable and/or did not benefit the FEHBP; and,
- \$70,787 (net) for unreturned health benefit refunds and recoveries.

Regarding the procedural finding, we determined that Florida Blue’s Special Investigations Unit is not in compliance with the:

- FEHBP contract;
- FEHBP Carrier Letters issued by OPM;
- guidance related to Fraud and Abuse Programs provided by the Association’s FEP Director’s Office; and,
- FEHBP’s requirement to notify OPM’s OIG of fraud and abuse cases.

As a result of Florida Blue’s non-compliance, fraud and abuse may go undetected and unreported within the FEHBP, thereby diminishing the overall effectiveness of this plan’s Fraud and Abuse Program.

The Association only agreed with \$383,983 of the questioned charges and generally disagreed with the procedural finding regarding Florida Blue’s Fraud and Abuse Program.

Florida Blue

JACKSONVILLE, FLORIDA

Report No. 1A-10-41-12-050

SEPTEMBER 10, 2013

Our audit of the FEHBP operations at Florida Blue covered miscellaneous health benefit payments and credits and cash management activities from 2010 through February 2012, as well as administrative expenses from 2009 through 2011. In addition, we



EMPLOYEE ORGANIZATION PLANS

Employee organization plans fall into the category of experience-rated plans. These plans either operate or sponsor participating Federal health benefits programs. As fee-for-service plans, they allow members to obtain treatment through facilities or providers of their choice.

The largest employee organizations are Federal employee unions and associations. Some examples are the: American Postal Workers Union; Association of Retirees of the Panama Canal Area; Government Employees Health Association, Inc.; National Association of Letter Carriers; National Postal Mail Handlers Union; and, Special Agents Mutual Benefit Association.

We did not issue any audit reports on employee organization plans during this reporting period.

EXPERIENCE-RATED COMPREHENSIVE MEDICAL PLANS

Comprehensive medical plans fall into one of two categories: community-rated or experience-rated. As we previously explained on page 1 of this report, the key difference between the categories stems from how premium rates are calculated.

Members of experience-rated plans have the option of using a designated network of providers or using out-of-network providers. A member's choice in selecting one health care provider over another has monetary and medical implications. For example, if a member chooses an out-of-network provider, the member will pay a substantial portion of the charges and covered benefits may be less comprehensive.

We issued one experience-rated comprehensive medical plan audit report during this reporting period for the Capital District Physicians' Health Plan.

Capital District Physicians' Health Plan

ALBANY, NEW YORK

Report No. 1D-SG-00-13-010

MAY 30, 2013

The Capital District Physicians' Health Plan (Plan) is an experience-rated health maintenance organization offering comprehensive health benefits to Federal enrollees and their families. Enrollment is open to all Federal employees and annuitants in the Plan's service area, which includes Upstate, Hudson Valley, and Central New York.

Our audit of the Plan's FEHBP operations covered miscellaneous health benefit payments and credits, such as refunds, fraud recoveries and pharmacy drug rebates, from 2007 through June 2012. In addition, we reviewed the Plan's cash management activities and practices related to FEHBP funds and the Plan's Fraud and Abuse Program from 2007 through June 2012.

Plan Agrees with \$10,168 for Lost Investment Income

Our auditors questioned \$10,168 for LII calculated on health benefit refunds and pharmacy drug rebates that were returned untimely to the FEHBP during the audit scope, and also identified a procedural finding regarding the Plan's annual fraud and abuse reports. The Plan agreed with the questioned LII amount and the procedural finding.



Information Systems Audits

OPM relies on computer technologies and information systems to administer programs that distribute health and retirement benefits to millions of current and former Federal employees. OPM systems also assist in the management of background investigations for Federal employees, contractors, and applicants as well as provide Government-wide recruiting tools for Federal agencies and individuals seeking Federal jobs. Any breakdowns or malicious attacks (e.g., hacking, worms, or viruses) affecting these Federal systems could compromise the privacy of the individuals whose information they maintain, as well as the efficiency and effectiveness of the programs that they support.

Our auditors examine the computer security and information systems of private health insurance carriers participating in the FEHBP by performing general and application controls audits. **General controls** refer to the policies and procedures that apply to an entity's overall computing environment. **Application controls** are those directly related to individual computer applications, such as a carrier's payroll system or benefits payment system. General controls provide a secure setting in which computer systems can operate, while application controls ensure that the systems completely and accurately process transactions. In addition, we are also responsible for performing an independent oversight of OPM's internal information technology and security program.

We perform an annual independent audit of OPM's information technology (IT) security environment, as required by the Federal Information Security Management Act of 2002 (FISMA). We also complete routine audits of OPM's major IT systems to ensure management has implemented appropriate security controls. When necessary, our auditors review system development projects to ensure adherence to best practices and disciplined system development lifecycle processes. During this reporting period we issued four final audit reports. Summaries of these audits are provided below.

Information Technology Security Controls for OPM's USA Staffing System

WASHINGTON, D.C.

Report No. 4A-HR-00-13-024

JUNE 21, 2013

The USA Staffing web-based application is a single integrated software solution, which enables staff in OPM's Human Resources Management group to design custom assessment tools, job application questionnaires, and job vacancy announcements for Government jobs.

The system is operated and hosted by the Human Resources Tools and Technology (HRTT) group in OPM's Office of the Chief Information Officer (OCIO).

Nothing came to our attention to indicate that HRTT is not in full compliance with FISMA requirements.

**No FISMA
Violations Were
Detected With
USA Staffing**



Information Technology Security Controls for OPM's Personnel Investigations Processing System

WASHINGTON, D.C.

Report No. 4A-IS-00-13-022

JUNE 24, 2013

We conducted an audit of OPM's Federal Investigative Services' (FIS) Personnel Investigations Processing System (PIPS). This system is used to process hundreds of thousands of background investigations annually and contains the OPM Security/Suitability Investigations Index. Approximately 15 million records of investigations conducted by and for OPM, the Federal Bureau of Investigations (FBI), the U.S. Department of State, the U.S. Secret Service, and other customer agencies are maintained in PIPS. Furthermore, the PIPS system interfaces with several other FIS systems to process applications while its data flow relies on both the OPM Local Area Network/Wide Area Network (LAN/WAN) and Enterprise Server Infrastructure (ESI) general support systems.

Our auditors reviewed the security of the PIPS and confirmed the OCIO assigned a PIPS Information System Security Officer (ISSO) to manage a variety of security functions. However, the most significant audit discovery revealed were deficient security controls for OPM's common controls catalog system.

OPM operates approximately 50 major systems that support the agency's mission. This includes three general support systems (GSS). A GSS is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people to leverage resources.

FISMA requires that all major information systems be subjected to security controls testing annually. When a security control is provided by GSS, there is no need for the controls to be independently tested by each system owner; rather, the owners of the GSS provide security control testing. These controls are referred to as common controls, and are said to be inherited by the individual major systems.

With FISMA in mind, the OPM OCIO created a common security controls catalog to be used as a shared resource by system owners to reduce duplicate testing. In addition to the controls provided by the GSSs, there are common controls addressed by agency-wide security policies, and by facilities management of various OPM buildings.

While the common security controls catalog offers a conceptually comprehensive approach to effectively using and testing a set of common security controls, the practical implementation of this catalog was flawed. In many cases, it did not accurately reflect the actual common controls provided by the OPM GSSs. Individual major system owners who relied on the common security controls catalog unknowingly believed that the GSS provided controls when, in fact, they did not. As a result of this flawed belief, individual system owners inappropriately omitted required security controls testing.

FIS Agrees with Audit Recommendations to Correct PIPS Security Control Deficiencies

In the case of PIPS, we found that there were a number of controls inappropriately labeled in the system security plan as common or inherited. As a result, these controls were never tested, increasing the risk that these controls may not be functioning as intended, and therefore posing a potential security threat to the system. This omission is particularly concerning given the purpose of the system and the nature of the data the system contains. Therefore in our final audit report, we recommended that the PIPS system owners work with the GSS owners to ensure that all controls in the PIPS system security plan are identified as being either common, inherited, hybrid, or system specific. Additionally, we further recommended that these controls be retested as soon as possible.

The PIPS system owners agreed with our recommendations and are taking the appropriate steps needed to address these concerns.



AUDIT ACTIVITIES

April 1, 2013 – September 30, 2013

Information Technology Security Controls for OPM's Serena Business Manager

WASHINGTON, D.C.

Report No. 4A-CI-00-13-023

JULY 19, 2013

Serena Business Manager (SBM) is one of OPM's critical IT systems. OPM's OCIO has ownership and managerial responsibility of the SBM system and is also responsible for IT development, support, and maintenance. SBM resides on the OPM LAN/WAN in the Development/Test and Production (DTP) environment.

SBM was originally purchased for software change management control and issue/defect tracking. After its acquisition, the OCIO realized that the software provided programmers the ability to develop

Serena Business Manager Security Concerns Addressed Through Corrective Action Plan

administrative applications for a fraction of the cost of purchasing customized software. There were many existing administrative support tracking

systems throughout OPM that were originally built using various technologies such as Microsoft Access, Powerbuilder, and Coldfusion. Reengineering these systems as SBM applications provided the OCIO an opportunity to build and maintain these applications in one environment where applications shared one browser interface, common software components, and one single place to manage user access and application security.

We have ongoing concerns about the security of SBM. The system was hacked twice last year, with both breaches resulting in a loss of sensitive data. We issued a flash audit alert to the OPM Director on April 8, 2013, to recommend that all public-facing elements of SBM be taken offline until the system is adequately secured.

In response to our alert, the Director instructed the OCIO to shut down the public-facing portion of the system. The OCIO also developed a corrective action plan to address the SBM security flaws. We agreed with the corrective action plan and are continuing to monitor this issue.

Information System General and Application Controls at BlueCross BlueShield of Tennessee

CHATTANOOGA, TENNESSEE

Report No. 1A-10-05-13-002

AUGUST 6, 2013

Our audit focused on the claims processing applications used to adjudicate FEHBP claims for BlueCross BlueShield of Tennessee (BCBST), as well as the various processes and IT systems used to support these applications. We documented controls in place and opportunities for improvement in each of the areas below.

Security Management

BCBST has established a series of IT policies and procedures to create an awareness of IT security. We also verified that BCBST has adequate policies related to the human resources security aspects of hiring, training, transferring, and terminating employees.

Access Controls

BCBST has implemented numerous controls to grant, remove, and control physical access to its data center, as well as logical controls to protect sensitive information. We also observed various controls over physical access to the facilities, as well as the method for encrypting emails containing sensitive information.

Network Security

BCBST has documented network infrastructure diagrams, implemented a secure firewall architecture, maintains comprehensive incident response policies and procedures, and utilizes software packages for incident correlation. However, BCBST's controls to detect rogue devices connected to its network could be improved.



Configuration Management

BCBST has developed formal policies and procedures that provide guidance for system software management and controlling configuration changes. However, we identified several weaknesses in BCBST's configuration management program related to system configuration auditing and its vulnerability scanning methodology.

Contingency Planning

We reviewed BCBST's business continuity plans and concluded that they contained the key elements

Control Weaknesses Cited in Configuration Management and Network Security

suggested by relevant guidance and publications. We also determined that these documents are reviewed and updated on a periodic basis.

Claims Adjudication

BCBST has implemented controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. We also determined that BCBST has adequate policies and procedures related to application change control.

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that BCBST is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.

Information System General and Application Controls at WellPoint Inc.

ROANOKE, VIRGINIA

Report No. 1A-10-00-13-012

SEPTEMBER 10, 2013

WellPoint Inc. (WellPoint) processes insurance claims for FEHBP members from twelve states enrolled in the BlueCross BlueShield Association's (BCBSA) Federal Employee Program. The scope of this audit examined the information systems used to process the BCBSA's

claims, as well as the various business processes and IT systems used to support these applications.

There was one element of our audit where WellPoint applied external interference with the application of audit procedures, resulting in our inability to fully comply with the Generally Accepted Government Auditing Standards requirement of independence. We routinely use our own automated tools to evaluate the configuration of a sample of computer servers. When we requested to conduct this test at WellPoint, we were informed that a corporate policy prohibited external entities from connecting to the WellPoint network. In an effort to meet our audit objective, we attempted to obtain additional information from WellPoint, but the Plan was unable to provide satisfactory evidence to confirm that it had a program in place to routinely monitor the configuration of its servers.

As a result of the scope limitation placed on our audit work and WellPoint's inability to provide additional supporting documentation, we are unable to independently attest that WellPoint's computer servers maintain a secure configuration.

In spite of the audit scope limitation, we were successful in documenting the controls in place and opportunities for improvement in each of the areas below.

Security Management

WellPoint has established a series of IT policies and procedures to make all company employees aware of their IT security responsibilities.

Access Controls

WellPoint has implemented numerous controls to grant and remove physical access to its data center, as well as logical controls to protect sensitive information. However, the physical access controls could be improved to one specific facility visited by our auditors. We also noted weaknesses in WellPoint's implementation of segregation of duties and privileged user monitoring.

Network Security

WellPoint has implemented a thorough incident response and network security program. However, we noted several opportunities for improvement



AUDIT ACTIVITIES

April 1, 2013 – September 30, 2013

related to WellPoint's network security controls.

WellPoint has not implemented technical controls to

WellPoint, Inc.'s Policy Resulted in a Scope Limitation

prevent rogue devices from connecting to its network. Also, several specific servers containing Federal data are

not subject to routine vulnerability scanning, and we could not obtain evidence indicating that these servers have ever been subject to a vulnerability scan. In addition, WellPoint limited our ability to perform adequate testing in this area of the audit.

Configuration Management

WellPoint has developed formal policies and procedures that provide guidance to ensure that system software is appropriately configured and updated, as well as for controlling system software configuration changes. However, we noted that WellPoint's mainframe password settings are not in compliance with its own corporate standards.

Contingency Planning

We reviewed WellPoint's business continuity plans and concluded that they contained the key elements suggested by relevant guidance and publications. We also determined that these documents are reviewed and updated on a periodic basis.

Claims Adjudication

WellPoint has implemented many controls in its claims adjudication process to ensure that FEHBP claims are processed accurately. However, we noted several weaknesses in WellPoint's claims application controls. Additionally, no auditing is performed to ensure the manual process for debarring providers is done appropriately.

Health Insurance Portability and Accountability Act (HIPAA)

Nothing came to our attention that caused us to believe that WellPoint is not in compliance with the HIPAA security, privacy, and national provider identifier regulations.



Internal Audits

OPM INTERNAL PERFORMANCE AUDITS

Our internal auditing staff focuses on improving the efficiency and effectiveness of OPM's operations and their corresponding internal controls. One critical area of this activity is the audit of OPM's consolidated financial statements required under the Chief Financial Officers (CFO) Act of 1990. Our staff also conducts performance audits covering other internal OPM programs and functions.

During this reporting period we issued one final internal audit report, which is summarized below.

Assessing the Relevance and Reliability of OPM's Performance Information

WASHINGTON, D.C.

Report No. 4A-CF-00-12-066

APRIL 1, 2013

We conducted a performance audit to assess the relevance and reliability of OPM's performance information. The objective of our audit was to determine if OPM has internal controls in place over the collection, review, and reporting of its performance information in the Annual Performance Report (APR). We reviewed performance information, as reported in the FY 2011 APR, for FIS and Retirement Services (RS) programs. In addition, we reviewed the RS claims backlog addressed in the RS Strategic Plan, dated January 2012.

For FIS, we reviewed the following performance measures:

- Requirements of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) for the average number of days to complete the fastest 90 percent of initial national security investigations, and,
- Number of investigations determined to be deficient due to errors in investigation processing.

In addition, we reviewed the performance measure developed by FIS to determine the percentage of customers satisfied with their quality and service products. We also reviewed FIS' policies and guidance. However, these results are not included in the FY 2011 APR because the customer satisfaction results were still being collected when the APR was published. At the time we performed our audit, these performance results were available for review.

For RS, we reviewed the following performance measures:

- Retirement claims processing timeliness;
- Average unit cost for processing retirement claims;
- Number of retirement records OPM receives that are complete and require no supplemental actions; and,
- Percent of customers satisfied with overall retirement services.

In addition, we reviewed OPM's progress in reducing the pending claims backlog as discussed in RS' FY 2012 Strategic Plan.

Our audit findings reveal that OPM needs to strengthen its controls over the collection, review, and reporting of performance information. Specifically, we found improvements are needed in the following areas:

- ***Change Control Procedures for Reporting Performance Measure Targets***
OPM has not established a change control process for performance targets reported in the Congressional Budget Justification and the APR.



AUDIT ACTIVITIES

April 1, 2013 – September 30, 2013

- ***Consistent Performance Indicators for Federal Investigative Services' Performance Measures***

Inconsistencies were found in OPM's reporting practices for investigative timeliness and deficient cases performance measures in the FY 2011 APR. In addition, the data used to determine the performance result for measuring deficient cases is not aligned with the performance measure definition.

- ***Improved Internal Controls to Report Retirement Services' Claims Backlog Status***

OPM does not have adequate controls in place to ensure proper tracking of retirement claims received and processed to determine and report the backlog status.

- ***Improved Internal Controls to Report Performance Results for the Retirement Claims Processing Timeliness***

OPM does not have adequate controls in place to ensure the accurate calculation of retirement claims processing timeliness. Specifically, OPM reports

that it processed non-disability retirement claims in an average of 125 days; however, OPM actually processed these claims in an average of 131 days.

OPM Needs to Strengthen its Controls over the Collection, Review, and Reporting of Performance Information in the APR

- ***Improved Internal Controls for the Performance Measures: Data Gathering, Reviewing, and Reporting of Customer Satisfaction***

OPM lacks adequate internal controls over the performance measures for data gathering, reviewing, and reporting of RS customer satisfaction.

OPM concurred with two of our recommendations, partially concurred with two recommendations, and did not concur with one recommendation.



Special Audits

In addition to health and life insurance, OPM administers various other benefit programs for Federal employees which include the: Federal Employees' Group Life Insurance (FEGLI) program; Federal Flexible Spending Account (FSAFEDS) program; Federal Long Term Care Insurance Program (FLTCIP); and, Federal Employees Dental and Vision Insurance Program (FEDVIP). Our office also conducts audits of Pharmacy Benefit Managers (PBMs) that coordinate pharmacy benefits for the FEHBP carriers. The objective of these audits is to ensure that costs charged and services provided to Federal subscribers are in accordance with the contracts and applicable Federal regulations. Additionally, our staff performs audits of the Combined Federal Campaign (CFC) to ensure that monies donated by Federal employees are properly handled and disbursed to charities according to the designations of contributing employees.

During this reporting period we issued one final audit report, which is summarized below.

Federal Employees Dental and Vision Insurance Program Operations as Administered by FEP BlueVision

CHICAGO, IL; LATHAM, NY;
AND SAN ANTONIO, TX

Report No. 1J-0C-00-13-025

SEPTEMBER 17, 2013

The Federal Employee Dental and Vision Benefits Enhancement Act of 2004, Public Law 108-496, 118 Statute 4001, was signed into law on December 23, 2004, and established a dental benefits and vision benefits program for Federal employees, annuitants, and their eligible family members. The FEDVIP carriers signed contracts with OPM to provide dental and vision insurance services for a term of seven years.

In August 2006, OPM awarded a contract to the BCBS Association to administer vision benefits under the FEDVIP. Pursuant to this contract, the BCBS Association provides contract oversight, field services for members, consumer education, reporting, and actuarial and financial services from its Chicago, Illinois, and Washington, D.C. locations. The BCBS Association's responsibilities for administering the

Plan under the contract are carried out by Davis Vision, a wholly owned subsidiary of Highmark, Inc., with locations in Latham, New York and San Antonio, Texas.

The BCBS Association's duties and responsibilities under the contract include, but are not limited to, the following:

- Providing payments or benefits to eligible members if they are entitled to FEDVIP benefits;
- Establishing internal procedures designed to expeditiously resolve disputes and include one or more alternative resolution procedures involving third-party review under appropriate circumstances by entities mutually acceptable to OPM and the carrier;
- Making vision benefits plan information available to eligible employees on services and benefits to facilitate their ability to make an informed decision about electing vision coverage;
- Maintaining and delivering accounting records and reports required by OPM; and,
- Assisting OPM and representatives of the Government Accountability Office (GAO) to examine carrier records whenever necessary to carry out the purposes of the contract.



AUDIT ACTIVITIES

April 1, 2013 – September 30, 2013

BCBS Association Working to Meet Performance Standards for Customer Service Inquiries

the BCBS Association's program responsibilities related to underwriting and price redeterminations,

During this reporting period, we issued a report on the Program's operations for the years 2008 through 2010. Specifically, the audit covered

cash management, administrative expenses, claims payments, compliance with performance standards, and fraud and abuse policies and procedures.

The audit identified one procedural finding that the BCBS Association did not meet all of the customer service performance standards to respond to written and email inquiries that were required by the Contract.

The BCBS Association continues to work with OPM to resolve this audit issue.



ENFORCEMENT ACTIVITIES

Investigative Cases

The Office of Personnel Management administers benefits from its trust funds, with approximately \$920 billion in assets for all Federal civilian employees and annuitants participating in the Civil Service Retirement System, the Federal Employees Retirement System, FEHBP, and FEGLI. These programs cover over eight million current and retired Federal civilian employees, including eligible family members, and disburse over \$100 billion annually. The majority of our OIG criminal investigative efforts are spent examining potential fraud against these trust funds. However, we also investigate OPM employee misconduct and other wrongdoing, such as fraud within the personnel security and suitability program administered by OPM.

During the reporting period, our office opened 27 criminal investigations and closed 28, with 96 still in progress. Our criminal investigations led to 18 arrests, 28 indictments and informations, 22 convictions and \$31,184,915 in monetary recoveries to OPM-administered trust funds. Our criminal investigations, many of which we worked jointly with other Federal law enforcement agencies, also resulted in \$233,603,050 in criminal fines and penalties, which are returned to the General Fund of the Treasury, asset forfeitures, and court fees and/or assessments. For a complete statistical summary of our office's investigative activity, refer to the table on page 27.

HEALTH CARE FRAUD

Health care fraud cases are often time-consuming and complex, and may involve several health care providers who are defrauding multiple health insurance plans. Our criminal and civil investigations are critical to protecting Federal employees, annuitants, and members of their families who are eligible to participate in the FEHBP. Of particular concern are the growth of medical identity theft and organized crime in health care fraud, which has affected the FEHBP.

We coordinate our health care fraud investigations with the Department of Justice (DOJ) and other Federal, state, and local law enforcement agencies. We are participating members of health care fraud task forces across the nation. We work directly with U.S. Attorney's Offices nationwide to focus investigative resources in areas where fraud is most prevalent.

Our special agents are in regular contact with FEHBP health insurance carriers to identify possible fraud by health care providers and enrollees. Additionally, special agents work closely with our auditors when fraud issues arise during carrier audits. They also coordinate with the OIG's debarment official when investigations of FEHBP health care providers reveal evidence of violations that may warrant administrative sanctions. The following investigative cases represent some of our activity during the reporting period.



ENFORCEMENT ACTIVITIES

April 1, 2013 – September 30, 2013

HEALTH CARE FRAUD CASES

FEHBP Recovers Over \$1 Million from Pediatrix Medical Group

In April 2013, Pediatrix Medical Group (Pediatrix), subsidiary of Mednax, Inc., and one of the nation's largest providers of newborn hearing screens, entered into a settlement agreement with the Government to pay \$2.2 million to resolve False Claims Act allegations. The allegations stemmed from the medical unbundling of labor and delivery charges for newborn hearing screenings from global hospital charges commonly referred to as Diagnosis-Related-Group (DRG) charges. Pediatrix incorrectly billed the government for newborn hearing screens by separately billing using Current Procedural Terminology Codes (CPT Codes). As a result, Pediatrix was improperly reimbursed for more compensation from Government Sponsored Programs and private insurance carriers directly from the hospital than they would have utilizing the DRG charges. In addition to the financial recovery, Pediatrix agreed not to submit held, pending, or future newborn hearing screening claims.

The FEHBP received \$1,008,889, which included lost investment income, as a result of the settlement. This allegation was proactively developed by our OIG/FEHBP Carrier Task Force's Proactive Working Group. The resulting investigation was conducted jointly with the Federal Bureau of Investigation (FBI), the Defense Criminal Investigative Service (DCIS), and our office.

Generic Drug Manufacturer Ranbaxy Pleads Guilty and Agrees to Pay \$500 Million to Resolve False Claims Allegations

In May 2013, a generic drug manufacturer, Ranbaxy USA Inc. (Ranbaxy), pled guilty to felony charges relating to the manufacture and distribution of certain adulterated drugs produced at two of its manufacturing facilities in India. Also Ranbaxy settled civil allegations that it submitted false claims to Federal health care programs.

The Federal Food, Drug and Cosmetic Act (FDCA) prohibits the introduction or delivery for introduction into interstate commerce any drug that is adulterated. Under FDCA definition, a drug is adulterated if the methods used in, or the facilities or controls used for its manufacturing, processing, packing, or holding do not conform to, or are not operated or administered in conformity with, current Good Manufacturing Practice (cGMP) regulations. This explanation assures that a specific drug will meet prescribed safety requirements in the drug's identity and strength, as well as meets the quality and purity characteristics, which the drug purports or is advertised to possess.

Additionally, Ranbaxy USA admitted to making false, fictitious, and fraudulent statements to the FDA in Annual Reports filed in 2006 and 2007 regarding the dates of stability tests conducted on certain batches of Cefaclor, Cefadroxil, Amoxicillin, and Clavulanate Potassium, which were manufactured at its Dewas facility.

The Federal government's share of the civil settlement amount is approximately \$232 million, and the remaining \$118 million will go to the states participating in the agreement.

The FEHBP received \$20,432,588 in this settlement and it was a joint OIG investigation conducted by the investigators from FDA, U.S. Agency for International Development (USAID), and our office.

Kmart Agrees to Pay \$2.5 Million to Resolve False Claims Allegations

In July 2013, Kmart entered into a settlement agreement with the United States Government pursuant to a qui tam. Kmart agreed to pay \$2.5 million to resolve False Claims Act allegations of billing full costs for prescriptions that were only partially filled or dispensed.

As a result of the settlement, the FEHBP received \$227,770.

This was a joint investigation with the HHS OIG and our office.



Trans 1 Violates the False Claims Act and Agrees to Pay \$6 Million Settlement

A medical device manufacturer, Trans 1, agreed to pay the United States \$6 million to resolve allegations that it violated the False Claims Act by allowing health care providers to submit false claims to Medicare and other Federal health care programs for minimally-invasive spine surgeries.

The settlement also resolves allegations that Trans 1:

- Knowingly caused health care providers to submit claims with incorrect diagnosis or procedure codes for certain minimally-invasive spine fusion surgeries in which physicians used Trans 1's AxiaLIF System™, a device developed as an alternative to invasive spine fusion surgeries;
- Improperly advised physicians and hospitals to use the incorrect billing codes for procedures designed for more invasive spinal fusion surgeries when they used the AxiaLIF System™ for less extensive medical techniques. As a result, health care providers received greater reimbursements than they were entitled to for performing the minimally-invasive AxiaLIF procedures; and,
- Promoted the sale of its AxiaLIF System™ for uses that were not approved by the U.S. Food and Drug Administration (FDA), including certain procedures to treat complex spinal deformity, which were not covered by Federal health care programs.

As a result of this settlement, the FEHBP will receive \$129,961. This was a joint investigation with the OIGs of HHS, DCIS, and our office.

Respi-Test Health Care Fraud Conviction Results in a \$4.7 Million Settlement

The owners of Respi-Test, Inc. (Respi-Test), a durable medical equipment provider located in North Carolina, were convicted of health care fraud. Respi-Test, Inc. provides home-based sleep study equipment and testing. The settlement involves allegations that Respi-Test devised a scheme to defraud private and Federal health insurers by billing for attended sleep studies, while merely performing

pulse oximetry testing. To get the claims paid, the owners also changed the diagnosis codes on claim forms and assumed the identity of a Medical doctor in order to give the appearance that the claims were medically necessary, supervised, and reviewed.

In July 2013, after pleading guilty, the owners were sentenced to imprisonment and restitution totaling \$4,782,570 of which the FEHBP will receive \$47,244.

This was a joint investigation with the HHS OIG and the OPM OIG.

Retired Federal Law Enforcement Officer Pleads Guilty to Forging Controlled Substance Prescriptions

A retired Federal Law Enforcement Officer (officer) forged prescriptions in his own name, assuming the identity of a Gastroenterologist to obtain controlled substances and submit false claims to the FEHBP.

Our investigation revealed that from June 2010 through October 2012, the officer forged 46 prescriptions for controlled substances, specifically Dilaudid, Roxicodone, Percocet, and Oxycontin. The officer created the prescriptions using reams of tamper-proof prescription paper he obtained from an online company. As a result of his activities, the officer fraudulently obtained 2,990 pills. The investigation further revealed that in 43 of the 46 fraudulent prescriptions, the officer purported himself to be a Gastroenterologist.

The 43 fraudulent claims resulted in losses to the Federal Government of approximately \$6,557. The remaining three prescriptions were paid in cash.

The officer agreed to waive indictment and plead guilty to health care fraud. The officer was sentenced to two years of probation and ordered to pay \$6,557 in restitution and fined \$5,000.

AMGEN Agrees to Pay \$24.9 Million to Resolve False Claims Allegations

In April 2013, AMGEN, a pharmaceutical manufacturer, entered into a settlement agreement with the Federal government, agreeing to pay \$24.9 million to resolve a False Claims Act violation. AMGEN agreed to resolve allegations it paid



ENFORCEMENT ACTIVITIES

April 1, 2013 – September 30, 2013

kickbacks to long-term care pharmacies and other health care providers in exchange for switching patients from a competitor drug to Aranesp, an AMGEN product. The investigation developed as a result of a civil complaint filed alleging that AMGEN engaged in the off label promotion of Aranesp in an attempt to increase its sales.

The FDA approved Aranesp to treat lower than normal red blood cells (anemia) caused by chronic kidney disease or chemotherapy. AMGEN began to promote Aranesp to long-term care pharmacies and other health care providers to treat patients that had not been diagnosed with anemia caused by either chronic renal failure or chemotherapy. AMGEN encouraged the non-approved FDA use (off-label use) of Aranesp by paying health care providers to promote off label uses and provided written materials to health care providers encouraging off-label uses of Aranesp.

As a result of the settlement the FEHBP received \$111,240.

This was a joint investigation conducted by the DCIS; the FBI; the FDA; the HHS OIG; and our office.

RETIREMENT FRAUD

Under the law, entitlement to annuity payments ceases upon the death of an annuitant or survivor annuitant (spouse). The most common type of retirement fraud involves the intentional receipt and use of Civil Service Retirement System (CSRS) or Federal Employees Retirement System (FERS) annuity benefit payments by an unentitled recipient. However, retirement fraud can also include incidents of elder abuse.

Our Office of Investigations uses a variety of approaches to identify potential retirement fraud cases for investigation. We coordinate closely with OPM's Retirement Services office to identify and address program vulnerabilities. We also coordinate with the Department of the Treasury's Financial Management Service to obtain payment information. Other referrals come from Federal, state, and local agencies, as well as private citizens. The OIG also works proactively to identify retirement fraud.

The following retirement fraud investigations represent some of our activities during the reporting period.

RETIREMENT FRAUD CASES

Son-in-law Steals Deceased Annuitant's Benefit Payments

We initiated this investigation in November 2012, after receiving allegations from the Social Security Administration (SSA) OIG that a son-in-law of a deceased Federal annuitant fraudulently obtained retirement payments from OPM. At the time of the referral, the SSA OIG was investigating the same individual for illegally cashing the annuitant's SSA benefits.

The Federal annuitant's benefit payments as well as his Social Security benefits were electronically deposited into a joint bank account shared by the annuitant and his son-in-law. The son-in-law admitted to withdrawing the money on a monthly basis after the annuitant died and using it to pay off credit card debt, various housing bills, and to pay his daughter's college tuition.

In April 2013, the son in law pled guilty to theft of public funds. In August 2013, he was sentenced and ordered to pay restitution in the amount of \$156,800 to OPM and \$31,765 to SSA.

This was a joint investigation by the SSA OIG and our office.

Daughter Conceals Mother's Death Collects Annuity Payments

We initiated this investigation after receiving allegations from the United States Secret Service (USSS) that a deceased survivor annuitant's daughter fraudulently obtained retirement payments from OPM. The survivor annuitant died in September 2004. Since OPM was never notified of the death, the annuity payments continued, resulting in an overpayment of \$77,379.

Our investigators determined that the survivor annuitant's daughter forged her mother's signature on three OPM address verification letters (AVLs), falsely certifying that her mother was still alive.

In May 2012, the daughter was convicted of theft of public funds and was sentenced in April 2013 to



8 months in prison, followed by 36 months of probation, and ordered to pay restitution to OPM in the amount of \$77,379 and to pay for her confinement in a community correction center.

This was a joint investigation conducted by the USSS and the OPM OIG.

Granddaughter Steals Deceased Grandmother's Survivor Annuity

We initiated this investigation after receiving allegations from the USSS that a deceased Federal survivor annuitant's granddaughter fraudulently obtained retirement payments from OPM. OPM was never notified of the survivor annuitant's death in June 2006.

The OPM survivor annuity payments were sent via electronic funds transfer to the bank account. For six years after her grandmother's death, the granddaughter collected her grandmothers' annuity benefits by writing checks on from the deceased annuitant's account. The granddaughter additionally changed the name from the bank account to her name. All of the checks written from the account were used by the granddaughter to pay for various personal expenses, including the building of a swimming pool and the purchase of a boat. It was determined that the granddaughter received over \$73,794 in improper benefits from OPM.

In April 2013, the granddaughter pled guilty to theft of public funds. In June 2013, she was sentenced to five years of supervised release. Additionally, the granddaughter was ordered to pay \$73,794 in restitution to OPM. The court also imposed a forfeiture order for all the funds held in her bank account, as well as her vehicle and boat.

This was a joint investigation conducted by the USSS and our office.

Deceased Mother's Survivor Annuity Stolen by Son

A survivor annuitant died in July 1998. OPM was not notified of the annuitant's death and payments continued to be deposited into her account until January 2007 resulting in an overpayment of \$88,051. This case was referred to us by OPM's Retirement Inspections in February 2009.

Our investigation revealed that one of the survivor annuitant's sons admitted to stealing the payments and the annuitant's other son admitted to knowing that his brother had not reported the death, knew he was using the payments, but claimed that he told him to stop several years prior.

In March 2013, the son, who gained access to improper benefits, pled guilty to theft of public money and was sentenced in August 2013. He was sentenced to 60 months of probation and ordered to pay \$88,051 in restitution to OPM.

Son Steals Deceased Annuitant's Benefits

This case was referred to the OIG by OPM's Retirement Inspections in August 2010. The case involves a Federal annuitant, who died in February 2002. Since OPM was not notified of the death, annuity payments continued resulting in an overpayment of \$340,291.

The payments were stopped in 2010 and the Federal annuitant's son called OPM to determine why payments were discontinued. Our investigators interviewed the son and he confessed to stealing the money. In December 2012, the son pled guilty to theft of public funds.

In June 2013, the son was sentenced to serve nine months incarceration; three years supervised release and to pay \$340,291 in restitution to OPM.

Theft of Deceased Annuitant's Benefits by Nephew

This case was referred to the OIG by OPM's Retirement Inspections in September 2010. The case involves a Federal annuitant, who died in January of 1992 and OPM was not notified of the death. Annuity payments continued resulting in an overpayment of \$130,843.

Our investigation revealed that a nephew was the informant on the death certificate. It further revealed that he forged the annuitant's name on at least two address verification letters (AVLs) sent by OPM to the annuitant causing continued retirement benefits to be paid.



ENFORCEMENT ACTIVITIES

April 1, 2013 – September 30, 2013

In September 2012, the nephew pled guilty to theft of public funds. In July 2013, he was sentenced to serve 15 months in prison, three years of supervised release, and to pay \$130,843 in restitution to OPM.

LIFE INSURANCE FRAUD CASE

Oldest Sibling Steals FEGLI Benefits from Other Siblings

The FEGLI Program contractor, MetLife, referred a case to our investigators in August 2011. Our investigation determined that a retired U.S. Postal Service employee, who died in August 2008, left a \$156,000.00 FEGLI insurance policy to be allocated equally to his four children. Each sibling was entitled to receive approximately \$39,000 in FEGLI benefits.

After interviewing the siblings and reviewing the case documentation, our investigators found that the oldest sibling forged the names of his two brothers and sister and stole a total of \$117,308 in FEGLI benefits to which he was not entitled. The oldest sibling contacted MetLife to have the check payments intended for his other siblings, redirected to his home address.

In February 2013, the brother pled guilty to making False Statements. He was sentenced to serve 18 months incarceration and ordered to pay \$117,308 in restitution to the FEGLI Program.

REVOLVING FUND PROGRAM INVESTIGATIONS

Our office investigates OPM employee misconduct and other wrongdoing, including allegations of fraud within OPM's revolving fund programs, such as the background investigations program and human resources products and services.

OPM's FIS conducts background investigations on Federal job applicants, employees, military members, and contractor personnel for suitability and security purposes. FIS conducts over 90 percent of all personnel background investigations for the Federal Government. With a staff of over 9,300 Federal and contract employees, FIS processed over 2.2 million

background investigations in FY 2012. Federal agencies use the reports of investigations conducted by OPM to determine individuals' suitability for employment and eligibility for access to national security classified information.

The violations investigated by our criminal investigators include fabrications by OPM background investigators (i.e., the submission of work products that purport to represent investigative work which was not in fact performed). We consider such cases to be a serious national security concern. If a background investigation contains incorrect, incomplete, or fraudulent information, a qualified candidate may be wrongfully denied employment or an unsuitable person may be cleared and allowed access to Federal facilities or classified information.

OPM's Human Resources Solutions (HRS) provides other Federal agencies, on a reimbursable basis, with human resource products and services to help agencies develop leaders, attract and build a high quality workforce, and transform into high performing organizations. For example, HRS operates the Federal Executive Institute, a residential training facility dedicated to developing career leaders for the Federal Government. Cases related to HRS investigated by our criminal investigators include employee misconduct, regulatory violations, and contract irregularities.

The following Revolving Fund investigations represent some of our activities during the reporting period.

Former OPM Background Investigator Sentenced for Falsifying Numerous Background Investigations

In November 2008, the OIG received an allegation from the FIS Integrity Assurance Group regarding misconduct and false statements made by an OPM Contract Background Investigator.

From January through July 2008, in more than two dozen background Reports of Investigations, the background investigator misrepresented that he had interviewed a source or reviewed a record regarding the subject of the background investigation, when in fact, he had not conducted an interview or obtained a record. These reports were utilized and relied upon by Federal agencies to determine whether these subjects



were suitable for positions having access to classified information, for positions impacting national security, or for receiving or retaining security clearances. These false representations required FIS to reopen and reinvestigate numerous background investigations assigned to the background investigator, which cost OPM \$78,832.

Our criminal investigators interviewed the background investigator, who admitted he randomly falsified reports, to include, personal testimony, and at least 20 source interviews associated with various background investigations. Additionally, the background investigator admitted, when he was initially notified of being under investigation for falsified reports, he made an attempt to conceal his false reporting by going to the residence of an individual source in an attempt to persuade the individual to lie when contacted by OPM investigators about being contacted by him as he had falsely reported.

In September 2013 the background investigator pled guilty and was sentenced to serve 180 days incarceration (suspended); 20 days community detention; 36 months of supervised probation, and ordered to pay full restitution of \$78,832 to OPM.

Former OPM Contract Background Investigator Sentenced for Falsifying Numerous Background Investigations

In April 2009, our office received an allegation from the FIS Integrity Assurance Group regarding misconduct and false statements made by an OPM Contract Background Investigator.

Between August 2006 and August 2007, in multiple background Reports of Investigations, the background investigator represented that he had interviewed a source or reviewed a record regarding the subject of the background investigation, when in fact, he had not conducted the interview or obtained the record. These reports were utilized and relied upon by Federal agencies requesting the background investigations to determine whether these subjects were suitable for positions having access to classified information, for positions impacting national security, or for receiving or retaining security clearances. These false representations required FIS to reopen and reinvestigate numerous background investigations assigned to the background investigator, costing OPM \$79,468.

After pleading guilty, the background investigator was sentenced in September 2013, to serve 60 days community detention; four years supervised probation; 200 hours of community service; and ordered by the court to pay restitution in the amount of \$79,468 to OPM.

OIG HOTLINE AND COMPLAINT ACTIVITY

The OIG's Fraud Hotline also contributes to identifying fraud and abuse. The Hotline telephone number, email address, and mailing address are listed on our OIG Web site at www.opm.gov/oig, along with an online anonymous complaint form. Contact information for the Hotline is also published in the brochures for all of the FEHBP health insurance plans. Those who report information to our Hotline can do so openly, anonymously, and confidentially without fear of reprisal.

The information we receive on our OIG Hotline generally concerns customer service issues, FEHBP health care fraud, retirement fraud, and other complaints that may warrant investigation. Our office receives inquiries from the general public, OPM employees, contractors and others interested in reporting waste, fraud, and abuse within OPM and the programs it administers.

We received 696 hotline inquiries during the reporting period, with 233 pertaining to health care and insurance issues, and 463 concerning retirement or special investigation. The table on page 27 reports the summary of hotline activities including telephone calls, emails, and letters.

OIG and External Initiated Complaints

Based on our knowledge of OPM program vulnerabilities, information shared by OPM program offices and contractors, and our liaison with other law enforcement agencies, we initiate our own inquiries into possible cases involving fraud, abuse, integrity issues, and occasionally malfeasance.

During this reporting period, we initiated 63 preliminary inquiry complaints related to retirement fraud and special investigations. We also initiated 541 health care fraud preliminary inquiry complaints. These efforts may potentially evolve into formal investigations.



ENFORCEMENT ACTIVITIES

April 1, 2013 – September 30, 2013

We believe that these OIG and external initiated complaints complement our hotline to ensure that our office continues to be effective in its role to guard against and identify instances of fraud, waste, and abuse.

Debarment Initiative Update

During the previous reporting period, the Inspector General's message discussed the agency's new Suspension and Debarment program, which became effective in March 2013. Prior to March 2013, the only active Suspension and Debarment Program at OPM was the OIG's Administrative Sanctions of FEHBP Health Care Providers. During this reporting period, the OIG referred 21 potential debarment cases to the agency, for a total of 22 referrals since the inception of the program. We recently learned that the OPM is pursuing its first two debarments. We have also requested reconsideration of our first eight debarment referrals, which were originally declined by the agency. All eight individuals in these cases were criminally

convicted former FIS employees or contractors. While they were removed from employment or from the relevant OPM contract, we feel a Government-wide debarment is needed to keep these individuals from obtaining similar employment at another Federal agency.

Our office will continue to develop and refer cases where we believe a government-wide debarment is necessary in order to protect the integrity of OPM, as well as other Federal agencies and programs.

Correction of Prior Period Semiannual Report

In our semiannual report for the period ending March 31, 2013, we underreported \$53,004 involving a health care investigation settlement. This underreporting occurred because the settlement amount owed the FEHBP Trust Fund was not calculated by DOJ until after the prior semiannual report was issued, therefore the amount was not available.



Administrative Sanctions of FEHBP Health Care Providers

Under the FEHBP administrative sanctions statute, we issue debarments and suspensions of health care providers whose actions demonstrate that they are not responsible to participate in the program. At the end of the reporting period, there were 32,477 active suspensions and debarments from the FEHBP.

During the reporting period, our office issued 418 administrative sanctions – including both suspensions and debarments – of health care providers who have committed violations that impact the FEHBP and its enrollees. In addition, we responded to 3,967 sanctions-related inquiries.

We develop our sanctions caseload from a variety of sources, including:

- Administrative actions issued against health care providers by other Federal agencies;
- Cases referred by the OIG's Office of Investigations;
- Cases identified by our office through systematic research and analysis of electronically-available information about health care providers, referred to as e-debarment; and,
- Referrals from other sources, including health insurance carriers and state Government regulatory and law enforcement agencies.

Sanctions serve a protective function for the FEHBP and the Federal employees who obtain, through it, their health insurance coverage. The following articles, highlighting a few of the administrative sanctions handled by our office during the reporting period, illustrate their value against health care providers who have placed the safety of enrollees at risk, or have obtained fraudulent payment of FEHBP funds.

Debarment disqualifies a health care provider from receiving payment of FEHBP funds for a stated period of time. The FEHBP administrative sanctions program establishes 18 bases for debarment. The ones we cite most frequently are for criminal convictions or professional licensure restrictions or

revocations. Before debarring a provider, our office gives prior notice and the opportunity to contest the sanction in an administrative proceeding.

Suspension has the same effect as a debarment, but becomes effective upon issuance, without prior notice or process. FEHBP sanctions law authorizes suspension only in cases where adequate evidence indicates that a provider represents an immediate risk to the health and safety of FEHBP enrollees.

The following is a summary of one of our debarment actions.

Arizona Physician Debarred After Medical Board Order Restricts License to Practice

Based on a referral from the Office of Investigations, we debarred an Arizona physician in May 2013. Our debarment was based on the Arizona Medical Board's (Board) decision to censor the physician and restrict his license to practice medicine for unprofessional conduct and gross patient negligence. On October 15, 2010, the Board filed an Order of Decree of Censure and Practice Restriction and Consent to the Same (Order) prohibiting the physician from prescribing, administering, or dispensing any Schedule II substances in any setting, for a period of five years.

The Board's Order cited the physician for unprofessional conduct or practice, and gross negligence in patient care; that is present or future care, which might be harmful or dangerous to the health of patients or the public. Specifically, the Board found



ENFORCEMENT ACTIVITIES

April 1, 2013 – September 30, 2013

that between 2003 and 2009, the physician failed to follow established medical treatment practices. The physician failed to:

- establish a formal goal-oriented treatment plan for his patients;
- perform periodic assessments of patients;
- enter into a pain treatment contract with patients;
- obtain and review patients' prior records;
- perform specific exams of a patient and consult with specialist regarding spine and chronic pain;
- coordinate and consult with pain management specialists and psychiatric specialists while treating a patient;
- perform comprehensive physical and neurological exams to confirm the legitimacy of one patient's pain;
- perform urine drug screening for patients who were prescribed large doses of pain medication; and,
- perform assessments of patients' depression.

The Board's findings referenced specific cases where the physician's continuous over-prescribing of controlled substances such as various opiates, benzodiazepines, and stimulants resulted in physical and psychological harm to his patients; and caused or contributed to the death of three patients.

Federal regulations state that the OPM may debar providers of health care services from participating in the FEHBP whose license to provide a health care service has been revoked, suspended, restricted, or not renewed, by a State licensing authority for reasons relating to the provider's professional competence, professional performance or financial integrity.

Our debarment of the physician is for an indefinite period pending the resolution of the physician's Arizona medical licensure restriction.

Ten Michigan Health Care Providers Suspended from the FEHBP

In September 2013, our office suspended six physicians and four pharmacists indicted in March 2013, by the grand jury of the United States District Court, Eastern District of Michigan Southern Division, for health care fraud and drug distribution. The ten health care providers were part of 44 individuals charged in a 13-count complaint that alleges that beginning on or about January 2008, an established group of physicians; pharmacists; pharmacy owners; home health care operators; and others; engaged in a conspiracy to defraud Government and private insurance companies.

Collectively, the group was charged with unlawful distribution and dispensing of various Schedule II, Schedule III, Schedule IV and Schedule V controlled substances; receiving kickbacks, bribes, money laundering, health care fraud, and other illegal benefits from the sale of drugs obtained by writing illegal prescriptions and fraudulent home health claims.

Medical practices and medical clinics were organized in multiple locations throughout Michigan and Ohio to engage in various aspects of the scheme. The group employed patient recruiters or patient marketers to obtain patients or patients personal information and directed them to one of the six doctors involved in the conspiracy. The doctors would sometimes perform a cursory examination; in most cases, the patient did not receive an examination nor had any physical contact with a physician. After the limited examination or exposure to the patient's information, the physician would then write prescriptions for controlled substances, directing the patient to have it filled at one of the pharmacies in their network. On other occasions the physician would sign blank prescriptions that would be completed later by some other individual involved in the group.

The patient recruiters or marketers presented the prescriptions to be filled, to one of the four pharmacists named in the indictment. The health care providers then billed the relevant insurers, as well as Medicare and Medicaid.

The indictment alleges that during the course of the conspiracy the group exploited private health insurance companies, Medicare, and Medicaid of over \$21.5 million.



The FEHBP administrative sanctions statute (statute) authorizes suspension of a health care provider when reliable evidence confirms a violation has occurred. In addition, the statute requires a need for immediate action to protect the health and safety of FEHBP beneficiaries.

All providers will remain suspended until a final disposition is made regarding the criminal charges pending against them.

California Physician Suspended for Unprofessional Conduct-Related Violations

In July 2013, we suspended a California, pediatric physician/surgeon from participating in the FEHBP. The suspension is based on the Medical Board of California's (Board) May 1, 2013, Ex Parte Interim Suspension Order (ISO) for violating the California Medical Practice Act.

The Board petitioned the State of California's Office of Administrative Hearings to immediately suspend the physician's medical license in order to protect the public's health, safety, and welfare. The Board's petition alleged that the physician was abusing controlled substances to the extent that she was a danger to herself and the public. The administrative judge determined that based on the evidence presented, the physician was unable to practice

safely due to violations of the California Medical Act and granted the Ex Parte ISO.

The Ex Parte ISO required the physician to refrain from practicing or attempting to practice any aspect of medicine until a determination was made in the Board's administrative hearing. In addition, Ex Parte ISO stipulates that the physician shall not:

- Possess; order; purchase; receive; furnish; administer or otherwise distribute controlled substances or dangerous drugs as defined by Federal or state law.
- Practice or advertise as available to practice medicine.
- Be present in any location or office which is maintained for the practice of medicine, or at which medicine is practiced for any purpose except as a patient or as a visitor of family or friends.

The Board presented its findings in an administrative hearing in June 2013 and granted an interim suspension order resulting in the suspension of the physician's California medical license. All of the terms and conditions of the May 1, 2013, Ex Parte ISO remain effective until either an accusation is issued and a decision is rendered, or the matter is resolved.

Our suspension is for an indefinite period pending the resolution of the physician's California medical licensure.



STATISTICAL SUMMARY OF ENFORCEMENT ACTIVITIES

Judicial Actions:

Arrests	18
Indictments and Informations	28
Convictions	22

Judicial Recoveries:

Restitutions and Settlements	\$31,184,915
Fines, Penalties, Assessments, and Forfeitures	\$233,603,050 ¹

Retirement and Special Investigations Hotline and Preliminary Inquiry Activity:

HOTLINE

Referred to:

OPM Program Offices	192
Other Federal Agencies	78
Informational Only	170
Inquiries Initiated	16
Retained for Further Inquiry	7
Total Received:	463

PRELIMINARY INQUIRY COMPLAINTS

Total Received:	63
Total Closed:	49

(Continued on next page)

¹This figure represents criminal fines and criminal penalties returned not to OPM, but to the general fund of the Treasury. It also includes asset forfeitures and court assessments and/or fees resulting from criminal investigations conducted by our office. Many of these criminal investigations were conducted jointly with other Federal agencies, who share the credit for the fines, penalties, assessments, and forfeitures.



STATISTICAL SUMMARY OF ENFORCEMENT ACTIVITIES

April 1, 2013 – September 30, 2013

Health Care Fraud Hotline and Preliminary Inquiry Complaint Activity:

HOTLINE

Referred to:

OPM Program Offices	58
FEHBP Insurance Carriers or Providers	76
Other Federal Agencies	13
Informational Only	69
Inquiries Initiated	7
Retained for Further Inquiry	10
Total Received:	233

PRELIMINARY INQUIRY COMPLAINTS

Total Received:	541
Total Closed:	514

Hotline Contacts and Preliminary Inquiry Complaints:

Total Hotline Contacts and Preliminary Inquiries Received:	1,300
Total Hotline Contacts and Preliminary Inquiries Closed:	1,242

Administrative Sanctions Activity:

FIS Cases Referred for Debarment and Suspension.	21
Health Care Debarments and Suspensions Issued	392
Health Care Provider Debarment and Suspension Inquiries	3,123
Health Care Debarments and Suspensions in Effect at End of Reporting Period.	32,257



APPENDICES

APPENDIX I-A Final Reports Issued with Questioned Costs for Insurance Programs APRIL 1, 2013 TO SEPTEMBER 30, 2013

Subject	Number of Reports	Dollar Value
A. Reports for which no management decision had been made by the beginning of the reporting period	0	\$ 0
B. Reports issued during the reporting period with findings	12	16,019,712
Subtotals (A+B)	12	16,019,712
C. Reports for which a management decision was made during the reporting period:	10	17,492,530
1. Disallowed costs	N/A	16,982,472
2. Costs not disallowed	N/A	510,058
D. Reports for which no management decision has been made by the end of the reporting period	2	(1,472,818) ²
E. Reports for which no management decision has been made within 6 months of issuance	0	0

²Represents the net costs, which includes overpayments and underpayments, to insurance carriers.



APPENDICES

April 1, 2013 – September 30, 2013

APPENDIX I-B Final Reports Issued with Questioned Costs for All Other Audit Entities APRIL 1, 2013 TO SEPTEMBER 30, 2013

Subject	Number of Reports	Dollar Value
A. Reports for which no management decision had been made by the beginning of the reporting period	4	\$67,948
B. Reports issued during the reporting period with findings	0	0
Subtotals (A+B)	4	67,948
C. Reports for which a management decision was made during the reporting period:	3	34,993
1. Disallowed costs	N/A	34,993
2. Costs not disallowed	N/A	0
D. Reports for which no management decision has been made by the end of the reporting period	1	32,955
E. Reports for which no management decision has been made within 6 months of issuance	1	32,955

APPENDIX II Final Reports Issued with Recommendations for Better Use of Funds APRIL 1, 2013 TO SEPTEMBER 30, 2013

Subject	Number of Reports	Dollar Value
A. Reports for which no management decision had been made by the beginning of the reporting period	1	\$10,000
B. Reports issued during the reporting period with findings	0	0
Subtotals (A+B)	1	10,000
C. Reports for which a management decision was made during the reporting period:	1	10,000
D. Reports for which no management decision has been made by the end of the reporting period	0	0
E. Reports for which no management decision has been made within 6 months of issuance	0	0



APPENDIX III
Insurance Audit Reports Issued
APRIL 1, 2013 TO SEPTEMBER 30, 2013

Report Number	Subject	Date Issued	Questioned Costs
1C-M9-00-12-056	MVP Health Care of Central Region in Schenectady, New York	April 1, 2013	\$ 2,723,833
1C-MX-00-12-064	MVP Health Care of Mid-Hudson Region in Schenectady, New York	April 9, 2013	272,646
1C-MS-00-13-014	Humana Health Plan, Inc. of Kansas City in Louisville, Kentucky	April 25, 2013	0
1C-P1-00-13-013	Aetna Open Access of Austin and San Antonio in Blue Bell, Pennsylvania	May 17, 2013	0
1C-E3-00-13-008	Kaiser Foundation Health Plan of the Mid-Atlantic States, Inc. in Rockville, Maryland	May 17, 2013	0
1D-SG-00-13-010	Capital District Physicians' Health Plan in Albany, New York	May 30, 2013	10,168
1C-HA-00-12-069	Coventry Health Care of Kansas, Inc. in Kansas City, Missouri	June 3, 2013	127,617
1C-59-00-13-028	Kaiser Foundation Health Plan, Inc. of Northern California in Burbank, California	July 3, 2013	0
1C-62-00-13-027	Kaiser Foundation Health Plan, Inc. of Southern California in Burbank, California	July 3, 2013	0
1C-EE-00-13-006	Humana Medical Plan, Inc. of South Florida in Louisville, Kentucky	July 10, 2013	101,227
1A-10-32-12-062	BlueCross BlueShield of Michigan in Detroit, Michigan	July 19, 2013	250,961
1C-51-00-13-039	Health Insurance Plan of Greater New York in New York, New York 2013 Proposed Rate Reconciliation	July 22, 2013	0
1C-QA-00-13-053	Independent Health Association – Plan Code QA in Buffalo, New York 2013 Proposed Rate Reconciliation	July 22, 2013	0
1C-MX-00-13-043	MVP Health Plan of Mid-Hudson Region in Schenectady, New York 2013 Proposed Rate Reconciliation	July 23, 2013	0



APPENDICES

April 1, 2013 – September 30, 2013

APPENDIX III Insurance Audit Reports Issued APRIL 1, 2013 TO SEPTEMBER 30, 2013 (Continued)

Report Number	Subject	Date Issued	Questioned Costs
1C-M9-00-13-059	MVP Health Plan of Central Region in Schenectady, New York 2013 Proposed Rate Reconciliation	August 5, 2013	\$ 619,932
1C-GA-00-13-057	MVP Health Plan of Eastern Region in Schenectady, New York 2013 Proposed Rate Reconciliation	August 5, 2013	(29,760)
1C-JP-00-13-031	MD Individual Practice Association, Inc. in Cypress, California	August 6, 2013	0
1A-99-00-13-004	Global Continuous Stay Claims for BlueCross and BlueShield Plans in Washington, D.C.	August 20, 2013	6,259,347
1A-10-41-12-050	Florida Blue in Jacksonville, Florida	September 10, 2013	1,768,338
1J-0C-00-13-025	Federal Employees Dental and Vision Insurance Program Operations as Administered by FEP Blue Vision for 2008 through 2010 in Chicago, Illinois and Latham, New York	September 17, 2013	0
1C-8W-00-13-040	UPMC Health Plan in Pittsburgh, Pennsylvania	September 23, 2013	0
1C-54-00-13-030	Group Health Cooperative in Spokane, Washington	September 26, 2013	0
1C-B9-00-13-020	United Healthcare of the Midwest, Inc. in Cypress, California	September 26, 2013	0
1C-P2-00-13-015	Presbyterian Health Plan in Albuquerque, New Mexico	September 26, 2013	1,933,916
1C-WJ-00-13-007	Group Health Cooperative of South Central Wisconsin in Madison, Wisconsin	September 26, 2013	1,981,487
TOTALS			\$16,019,712



APPENDIX IV

Internal Audit Reports Issued

APRIL 1, 2013 TO SEPTEMBER 30, 2013

Report Number	Subject	Date Issued
4A-CF-00-12-066	Assessing the Relevance and Reliability of the U.S. Office of Personnel Management's Performance Information in Washington, D.C.	April 1, 2013

APPENDIX V

Information Systems Audit Reports Issued

APRIL 1, 2013 TO SEPTEMBER 30, 2013

Report Number	Subject	Date Issued
4A-HR-00-13-024	Information Technology Security Controls of OPM's USA Staffing System in Washington, D.C.	June 21, 2013
4A-IS-00-13-022	Information Technology Security Controls of OPM's Investigations Processing System in Washington, D.C.	June 24, 2013
4A-CI-00-13-023	Information Technology Security Controls of OPM's Serena Business Manager in Washington, D.C.	July 19, 2013
1A-10-15-13-002	Information Systems General and Application Controls at BlueCross BlueShield of Tennessee in Chattanooga, Tennessee	August 6, 2013
1A-10-00-13-012	Information Systems General and Application Controls at WellPoint Inc. in Roanoke, Virginia	September 10, 2013



APPENDICES

April 1, 2013 – September 30, 2013

APPENDIX VI Summary of Audit Reports More Than Six Months Old Pending Corrective Action APRIL 1, 2013 TO SEPTEMBER 30, 2013

Report Number	Subject	Date Issued
4A-CF-00-05-028	Administration of the Prompt Payment Act at OPM in Washington, D.C.; 12 total recommendations; 2 open recommendations	April 16, 2007
4A-CI-00-08-022	Federal Information Security Management Act for Fiscal Year 2008 in Washington, D.C.; 19 total recommendations; 3 open recommendations	September 23, 2008
4A-CF-00-08-025	OPM's Fiscal Year 2008 Consolidated Financial Statement in Washington, D.C.; 6 total recommendations; 1 open recommendation	November 14, 2008
4A-CI-00-09-031	Federal Information Security Management Act for Fiscal Year 2009 in Washington, D.C.; 30 total recommendations; 3 open recommendations	November 5, 2009
4A-CF-00-09-037	OPM's Fiscal Year 2009 Consolidated Financial Statement in Washington, D.C.; 5 total recommendations; 1 open recommendation	November 13, 2009
4A-IS-00-09-060	Quality Assurance Process Over Background Investigations in Washington, D.C.; 18 total recommendations; 1 open recommendation	June 22, 2010
4A-CF-00-10-015	OPM's Fiscal Year 2010 Consolidated Financial Statement in Washington, D.C.; 7 total recommendations; 3 open recommendations	November 10, 2010
4A-CI-00-10-019	Federal Information Security Management Act for FY 2010 in Washington, D.C.; 41 total recommendations; 4 open recommendations	November 10, 2010
4A-CF-00-10-043	Payroll Debt Management Process for Active and Separated Employees in Washington, D.C.; 8 total recommendations; 1 open recommendation	March 4, 2011
4A-CI-00-11-016	Information Technology Security Controls for OPM's Enterprise Server Infrastructure General Support System in Washington, D.C.; 3 total recommendations; 2 open recommendations	May 16, 2011
1K-RS-00-11-068	Stopping Improper Payments to Deceased Annuitants in Washington, D.C.; 14 total recommendations; 4 open recommendations	September 14, 2011
4A-CI-00-11-009	Federal Information Security Management Act for Fiscal Year 2011 in Washington, D.C.; 29 total recommendations; 7 open recommendations	November 9, 2011



APPENDIX VI
Summary of Audit Reports More Than Six Months Old
Pending Corrective Action
APRIL 1, 2013 TO SEPTEMBER 30, 2013

(Continued)

Report Number	Subject	Date Issued
4A-CF-00-11-050	OPM's Fiscal Year 2011 Consolidated Financial Statement in Washington, D.C.; 7 total recommendations; 1 open recommendation	November 14, 2011
1A-99-00-11-022	Global Duplicate Claim Payments for BlueCross and BlueShield Plans in Washington, D.C.; 3 total recommendations; 1 open recommendation	January 11, 2012
4A-RI-00-12-034	Insecure Password Reset Process on Agency-owned Information Systems in Washington, D.C.; 3 total recommendations; 1 open recommendation	February 7, 2012
1B-31-00-10-038	Government Employees Health Association, Inc. in Lee's Summit, Missouri; 16 total recommendations; 7 open recommendations	March 12, 2012
1A-99-00-11-055	Global Coordination of Benefits for BlueCross and BlueShield Plans in Washington, D.C.; 6 total recommendations; 1 open recommendation	March 28, 2012
4A-CF-00-09-014	OPM's Interagency Agreement Process in Washington, D.C.; 8 total recommendations; 6 open recommendations	March 28, 2012
1A-99-00-12-001	Global Omnibus Budget Reconciliation Act of 1993 Claims for BlueCross and BlueShield Plans in Washington, D.C.; 6 total recommendations; 2 open recommendations	July 16, 2012
4A-OP-00-12-013	Information Technology Security Controls of OPM's Audit Report and Receivables Tracking System in Washington, D.C.; 24 total recommendations; 21 open recommendations	July 16, 2012
4A-HR-00-12-037	Information Security Posture of OPM's USAJOBS System in Washington, D.C.; 26 total recommendations; 1 open recommendation	July 26, 2012
1B-31-00-11-066	Information Systems General and Application Controls at Government Employees Health Association, Inc. in Lee's Summit, Missouri; 26 total recommendations; 10 open recommendations	August 9, 2012
4A-CF-00-12-015	Information Technology Security Controls of OPM's Service Credit Redeposit and Deposit System in Washington, D.C.; 9 total recommendations; 1 open recommendation	August 9, 2012
4A-CF-00-11-067	Administration of the Prompt Payment Act at OPM in Washington, D.C.; 12 total recommendations; 9 open recommendations	September 13, 2012



APPENDICES

April 1, 2013 – September 30, 2013

APPENDIX VI Summary of Audit Reports More Than Six Months Old Pending Corrective Action

APRIL 1, 2013 TO SEPTEMBER 30, 2013

(Continued)

Report Number	Subject	Date Issued
4A-CI-00-12-016	Federal Information Security Management Act for FY 2012 in Washington, D.C.; 18 total recommendations; 11 open recommendations	November 5, 2012
4A-CF-00-12-039	OPM's Fiscal Year 2012 Consolidated Financial Statement in Washington, D.C.; 3 total recommendations; 1 open recommendation	November 15, 2012
1D-80-00-12-045	Information Systems General and Application Controls at EmblemHealth in New York, New York; 12 total recommendations; 4 open recommendations	December 10, 2012
1K-RS-00-12-031	OPM's Voice over the Internet Protocol Phone System Interagency Agreement with the District of Columbia in Washington, D.C.; 2 total recommendations; 2 open recommendations	December 12, 2012
1A-10-33-12-020	BlueCross BlueShield of North Carolina in Durham, North Carolina; 10 total recommendations; 1 open recommendation	December 27, 2012
1A-10-67-12-004	BlueShield of California in San Francisco, California; 13 total recommendations; 5 open recommendations	January 10, 2013
1A-99-00-12-055	Global Assistant Surgeon Claim Overpayments for BlueCross and BlueShield Plans in Washington, D.C.; 3 total recommendations; 2 open recommendations	February 21, 2013
4A-CF-00-13-016	OPM's Fiscal Year 2012 Improper Payments Reporting for Compliance with the Improper Payments Elimination and Recovery Act of 2010 in Washington, D.C.; 1 total recommendation; 1 open recommendation	March 11, 2013
1C-22-00-12-065	Information Systems General and Application Controls at Aetna Inc. in Hartford, Connecticut; 9 total recommendations; 8 open recommendations	March 18, 2013
1A-99-00-12-029	Global Coordination of Benefits for BlueCross and BlueShield Plans in Washington, D.C.; 7 total recommendations; 6 open recommendations	March 20, 2013



APPENDIX VII

Most Recent Peer Review Results

APRIL 1, 2013 TO SEPTEMBER 30, 2013

We do not have any open recommendations to report from our peer reviews.

Subject	Date of Report	Result
System Review Report for the U.S. Office of Personnel Management's Office of the Inspector General Audit Organization <i>(Issued by the Office of Inspector General, Board of Governors of the Federal Reserve System)</i>	September 26, 2012	Pass ³
Quality Control System Review of the U.S. Department of Commerce's Office of Inspector General Audit Organization <i>(Issued by the Office of the Inspector General, U.S. Office of Personnel Management)</i>	July 13, 2012	Pass ³
Quality Assessment Review of the Investigative Operations of the Office of the Inspector General for the U.S. Office of Personnel Management <i>(Issued by the Office of Inspector General, U.S. Department of State)</i>	June 21, 2013	Compliant ⁴

³A peer review rating of **Pass** is issued when the reviewing Office of Inspector General concludes that the system of quality control for the reviewed Office of Inspector General has been suitably designed and complied with to provide it with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The Peer Review does not contain any deficiencies or significant deficiencies.

⁴A rating of **Compliant** conveys that the reviewed Office of Inspector General has adequate internal safeguards and management procedures to ensure that the Council of the Inspectors General on Integrity and Efficiency standards are followed and that law enforcement powers conferred by the 2002 amendments to the Inspector General Act are properly exercised.



APPENDICES

April 1, 2013 – September 30, 2013

APPENDIX VIII Investigative Recoveries APRIL 1, 2013 TO SEPTEMBER 30, 2013

OIG Case Number ⁵	Case Category	Action ⁵	OPM Recovery (Net)	Total Recovery (All Programs/ Victims)	Fines, Penalties, Assessments, and Forfeitures
I-12-00310	Federal Investigative Services Fraud	Administrative	\$ 298,410	\$ 298,410	\$ 0
I-12-00331	Federal Investigative Services Fraud	Administrative	150,369	150,369	0
I 2009 00021	Federal Investigative Services Fraud	Criminal	78,833	78,833	50
I 2010 00064	Federal Investigative Services Fraud	Criminal	79,467	79,467	100
TOTAL	Federal Investigative Services Fraud		\$ 607,079	\$ 607,079	\$ 150
I 2007 00499	Health Care Fraud	Civil	2,845,525	257,400,000	0
I 2008 00079	Health Care Fraud	Civil	227,700	2,550,000	0
I 2009 00047	Health Care Fraud	Civil	20,436	3,100,000	0
I 2010 00522	Health Care Fraud	Civil	8,777	750,000	0
I 2010 00865	Health Care Fraud	Civil	19,232	1,000,000	0
I 2010 00872	Health Care Fraud	Civil	20,432,587	350,000,000	0
I 2010 00939	Health Care Fraud	Civil	103,119	14,500,000	0
I 2011 00028	Health Care Fraud	Civil	3,482,203	17,468,777	0
I 2011 00403	Health Care Fraud	Civil	38,746	242,204	0
I 2011 00575	Health Care Fraud	Civil	978,622	1,008,889	0
I 2011 00814	Health Care Fraud	Civil	111,240	24,900,000	0
I-12-00319	Health Care Fraud	Civil	115,639	2,550,000	0
I-12-00339	Health Care Fraud	Civil	129,961	6,000,000	0
I-12-00408	Health Care Fraud	Civil	1,404	1,363,636	0
I 2007 00104	Health Care Fraud	Criminal	0	4,769	50
I 2007 00104	Health Care Fraud	Criminal	0	26,536	100
I 2007 00499	Health Care Fraud	Criminal	0	0	233,584,125
I 2010 00032	Health Care Fraud	Criminal	9,660	29,944	10,025
I 2010 00085	Health Care Fraud	Criminal	0	0	100
I 2010 00085	Health Care Fraud	Criminal	47,244	4,782,570	100
I 2011 00503	Health Care Fraud	Criminal	10,065	10,065	100
I 2011 00673	Health Care Fraud	Criminal	0	0	700
I-13-00148	Health Care Fraud	Criminal	6,557	6,557	5,200
TOTAL	Health Care Fraud		\$28,588,717	\$687,693,947	\$233,600,500



APPENDIX VIII

Investigative Recoveries

APRIL 1, 2013 TO SEPTEMBER 30, 2013

(Continued)

OIG Case Number ⁵	Case Category	Action ⁵	OPM Recovery (Net)	Total Recovery (All Programs/Victims)	Fines, Penalties, Assessments, and Forfeitures
I 2011 00068	Life Insurance Fraud	Criminal	\$117,308	\$117,308	\$ 100
TOTAL	Life Insurance Fraud		\$117,308	\$117,308	\$ 100
I 2011 00049	Retirement Fraud	Administrative	108,369	108,369	0
I 2009 00083	Retirement Fraud	Criminal	406,026	406,026	100
I 2010 00074	Retirement Fraud	Criminal	88,051	88,051	100
I 2011 00001	Retirement Fraud	Criminal	398,774	398,774	100
I 2011 00013	Retirement Fraud	Criminal	77,379	77,379	500
I 2011 00024	Retirement Fraud	Criminal	130,843	130,843	100
I 2011 00046	Retirement Fraud	Criminal	340,291	340,291	100
I-12-00674	Retirement Fraud	Criminal	73,794	73,794	100
I-13-00169	Retirement Fraud	Criminal	156,800	188,565	1,100
I-13-00217	Retirement Fraud	Criminal	91,484	346,522	100
TOTAL	Retirement Fraud		\$1,871,811	\$2,158,614	\$ 2,300
GRAND TOTAL			\$31,184,915	\$690,576,948	\$233,603,050

⁵Cases that are listed multiple times indicate there were multiple subjects.



INDEX OF REPORTING REQUIREMENTS

(Inspector General Act of 1978, As Amended)

	Page
Section 4 (a) (2): Review of legislation and regulations	No Activity
Section 5 (a) (1): Significant problems, abuses, and deficiencies	1-25
Section 5 (a) (2): Recommendations regarding significant problems, abuses, and deficiencies.	1-14
Section 5 (a) (3): Recommendations described in previous semiannual reports on which corrective action has not been completed	No Activity
Section 5 (a) (4): Matters referred to prosecutive authorities	15-25
Section 5 (a) (5): Summary of instances where information was refused during this reporting period	No Activity
Section 5 (a) (6): Listing of audit reports issued during this reporting period.	31-33
Section 5 (a) (7): Summary of particularly significant reports	1-25
Section 5 (a) (8): Audit reports containing questioned costs	29-30
Section 5 (a) (9): Audit reports containing recommendations for better use of funds	30
Section 5 (a) (10): Summary of unresolved audit reports issued prior to the beginning of this reporting period	34-36
Section 5 (a) (11): Significant revised management decisions during this reporting period	No Activity
Section 5 (a) (12): Significant management decisions with which the OIG disagreed during this reporting period	No Activity
Section 5 (a) (14) (A): Peer reviews conducted by another OIG	37
Section 5 (a) (16): Peer reviews conducted by the OPM OIG	No Activity



OIG HOTLINE

Report Fraud, Waste or Abuse to the Inspector General

Please Call the HOTLINE:

202-606-2423

Toll-free HOTLINE:

877-499-7295

Caller can remain anonymous • Information is confidential

<http://www.opm.gov/oig/html/hotline.asp>



MAILING ADDRESS:

OFFICE OF THE INSPECTOR GENERAL
U.S. Office of Personnel Management

Theodore Roosevelt Building

1900 E Street, N.W.

Room 6400

Washington, DC 20415-1100



Office of the Inspector General

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Theodore Roosevelt Building | 1900 E Street, N.W., Room 6400 | Washington, DC 20415-1100

Telephone: (202) 606-1200 | Fax: (202) 606-2153

Web Site: www.opm.gov/oig

SEPTEMBER 2013
OIG-SAR-49