U.S. OFFICE OF PERSONNEL MANAGEMENT

OFFICE OF THE INSPECTOR GENERAL

SEMIANNUAL REPORT TO CONGRESS

April 1, 2019–September 30, 2019

Productivity Indicators

FINANCIAL IMPACT	
Audit Recommendations for Recovery of Funds	$27,805,879
Management Commitments to Recover Funds	$6,105,734
Recoveries through Investigative Actions	$20,224,044

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	16
Evaluation Reports Issued	1
Management Advisories Issued	0
Investigations and Complaints Closed	325
Indictments and Informations	56
Arrests	42
Convictions	56
Hotline Contacts and Complaints Received	1,339
Hotline Contacts and Complaints Closed	1,085
FEHBP Provider Debarments and Suspensions	489
FEHBP Provider Debarment and Suspension Inquiries	2,053

Message from the Deputy Inspector General

In September 2019, the United States Senate confirmed Dale Cabaniss as the new Director of the U.S. Office of Personnel Management (OPM). We welcome Director Cabaniss at a time that is a defining moment in OPM's history. Director Cabaniss has an opportunity to lead the agency in fulfilling its potential by properly investing in technology and the Office of the Chief Information Officer (OCIO). The Office of the Inspector General (OIG) will continue to independently review OPM's efforts to manage its technology in furtherance of the OIG's mission to promote integrity, economy, and effectiveness of OPM's programs and operations.

Recently, OPM has been characterized as "not only failing in technology, it's failing in its core mission."[1] Although we have been critical of OPM's information technology (IT) operations and security program, we do not believe that OPM technology is "failing," or that OPM has not delivered core services to its customers and stakeholders. In fact, OPM should be credited with continuing to carry out its mission while facing significant challenges.

There is no denying that OPM's business processes are less efficient than they could be if they were supported by modern technology. For example, retirement annuity claims processing requires too much manual intervention because the legacy technology does not support the complex business rules associated with Federal retirement. Despite these limitations, OPM's average time to process a retirement claim, over the past two fiscal years (FYs), has consistently been under the goal of 60 days and it successfully processes monthly annuity payments to 2.7 million Federal annuitants.

Director Cabaniss has an opportunity to change the organizational culture regarding IT modernization. For many years, OPM has not properly invested in technology. The OCIO has been chronically understaffed and does not have appropriate authority and control over the IT budget in the agency.[2] OPM also suffers from a "shadow IT" problem – a term that refers to IT applications and infrastructure that are managed and used outside the control of the enterprise IT department. This is problematic because if an organization's Chief Information Officer (CIO) does not control the funding and technology, there cannot be an effective IT enterprise architecture.[3] A mature enterprise architecture is the hallmark of high performing, responsive, and cost-effective IT operations.

1 Testimony of former OPM Acting Director Margaret Weichert, appearing before the House Committee on Oversight and Reform Government Operations Subcommittee (May 21, 2019).

2 As reported in our FY 2018 FISMA Audit Report, 4A-CI-00-18-038, and our FITARA Audit Report, 4A-CI-00-18-037.

3 Enterprise architecture refers to a unified IT environment with standardized hardware and software designed to meet the strategic business needs of the organization.

However, we are encouraged by the fact that OPM's current OCIO leadership team has a background in private sector modernization initiatives. The OCIO leadership has skillfully articulated their understanding of these challenges and have a vision to lead the agency's IT modernization forward. Importantly, they have built transparency and accountability into the IT modernization planning process. The CIO's current plan involves modernizing OPM's mainframe computers, rewriting mission critical legacy applications, and redesigning the OCIO organization to introduce best practices from the private sector.

Nonetheless, OPM's mainframe computer environment poses considerable risk to the agency. High value mainframe applications supporting core OPM functions are outdated and overly integrated. The mainframe computers are physically located in an obsolete data center. However, the OCIO has already made significant progress with modernizing the mainframe environment by purchasing new computers and moving them into a commercial data center. There is also a solid plan and some movement to detangle legacy mainframe applications and position the agency to adopt modern application development techniques. While these are very positive developments, success managing OPM's IT systems will require sufficient strategic investment in resources. It is also essential that OPM adopt a capital planning and investment control (CPIC) process following the Office of Management and Budget budgetary guidance. Historically, OPM has struggled with the CPIC process, as we have documented in several of our Inspector General audit reports.[4] Fortunately, the current OCIO leadership seems to understand the right approach and has identified that estimating costs of modernizing applications and creating a cost accounting model are a critical part of its modernization strategy for FY 2020.

We look forward to working with Director Cabaniss on addressing the challenge of modernizing the OPM IT systems. Empowering and adequately funding the OCIO to carry out this IT modernization vision will support OPM's mission critical programs, including Retirement and the Federal Employees Health Benefits Program. We believe that with a robust IT environment, the dedicated OPM personnel will have the opportunity to more efficiently, effectively, and securely fulfill OPM's core mission. Finally, the OIG will continue our critical oversight role and independently monitor OPM's IT modernization efforts, in accordance with the OIG's statutory mission to promote the efficiency and effectiveness of OPM's programs and operations.

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

4 Flash Audit Alert - U.S. Office of Personnel Management's Infrastructure Improvement Project, 4A-CI-00-15-055; Fiscal Year 2017 Modernization Expenditure Plan, 4A-CI-00-18-022; and Fiscal Year 2018 Modernization Expenditure Plan, 4A-CI-00-18-044.

Mission Statement

Mission

To provide independent and objective oversight of OPM programs and operations.

Vision

Oversight through innovation.

Core Values

Vigilance
Safeguard OPM's programs and operations from fraud, waste, abuse, and mismanagement.

Integrity
Demonstrate the highest levels of professionalism, independence, and quality in our work and operations.

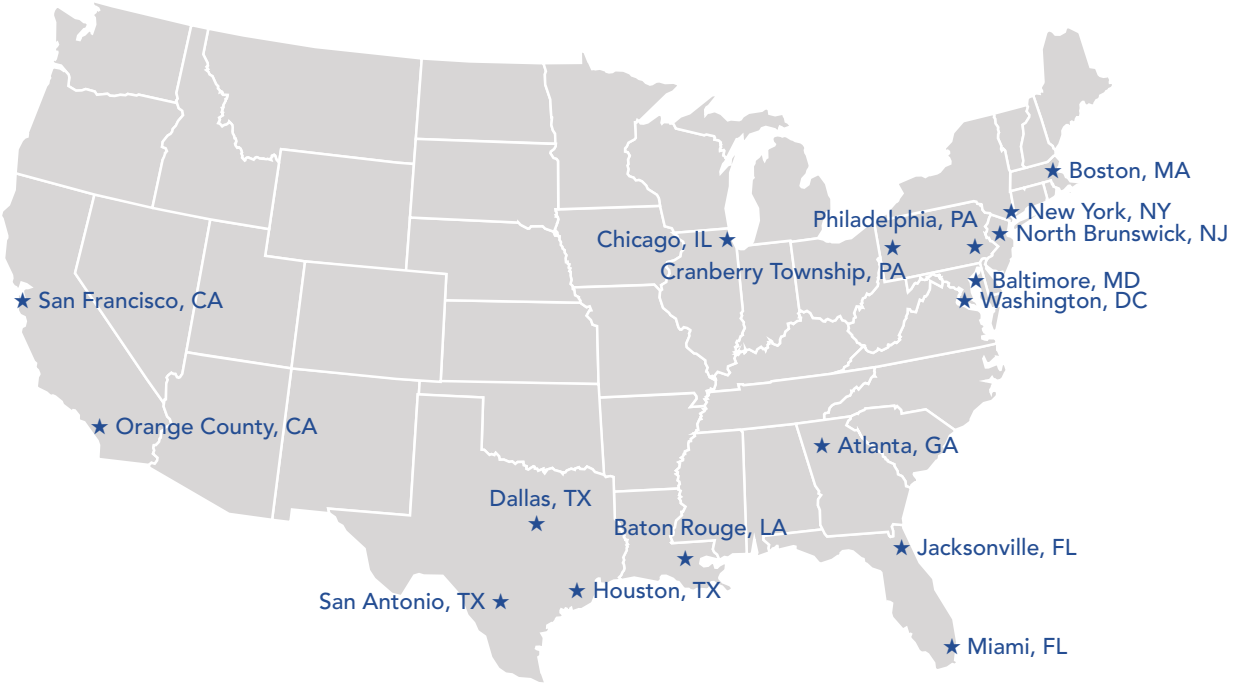
Empowerment
Emphasize our commitment to invest in our employees and promote our effectiveness.

Excellence
Promote best practices in OPM's management of program operations.

Transparency
Foster clear communication with OPM leadership, Congress, and the public.

Table of Contents

Field Offices



Audit Activities

Health Insurance Carrier Audits

The U.S. Office of Personnel Management (OPM) contracts with Federal Employee Health Benefits Program (FEHBP) carriers for health benefit plans for Federal employees and their eligible family members. The Office of Audits is responsible for auditing the activities of these health plans to ensure that they meet their contractual obligations with OPM. The selection of specific audits to conduct each year is based on a risk assessment model that considers various factors, including the size of the health insurance carrier, the time elapsed since the last audit, and our previous audit results.

The Office of the Inspector General's (OIG) insurance audit universe encompasses over 200 audit sites, consisting of health insurance carriers, sponsors, and underwriting organizations participating in the FEHBP. The number of audit sites fluctuates due to the addition, non-renewal, and merger of participating health insurance carriers. Combined premium payments for the health insurance program total over $50 billion annually. The health insurance plans that our office audits are classified as either community-rated or experience-rated carriers.

Community-rated carriers offer comprehensive medical plans, commonly referred to as health maintenance organizations (HMOs). They are responsible for paying claims and administrative costs incurred, and are paid an amount commensurate with the number of subscribing FEHBP members and the premiums paid by those members. Consequently, community-rated carriers suffer the loss if the costs incurred by the plan exceed the amount of premiums received.

Experience-rated carriers offer mostly fee-for-service plans (the largest being the Blue Cross and Blue Shield (BCBS) Service Benefit Plan), but also offer experience-rated HMOs. These carriers are reimbursed for actual claims paid and administrative expenses incurred, and paid a service charge that is determined in negotiation with OPM. Experience-rated carriers may suffer a loss in certain situations if claims exceed amounts available in the Employee Health Benefits Fund, which is a fund in the U.S. Treasury that holds premiums paid by members and from which carriers are reimbursed for claims incurred.

During the current reporting period, we issued seven final audit reports on health plans participating in the FEHBP, which contained recommendations for the return of over $27 million to the OPM-administered trust fund or the medical loss ratio (MLR) penalty fund.

Community-Rated Carriers

The community-rated carrier audit universe includes approximately 150 health plans located throughout the country. Community-rated audits are designed to ensure that the premium rates health plans charge the FEHBP are in accordance with their respective contracts and applicable Federal laws and regulations.

Similarly Sized Subscriber Group Audits

Federal regulations effective prior to July 2015 required that the FEHBP rates be equivalent to the rates a health 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 health 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.

SSSGs audits of traditional community-rated carriers focus on ensuring that:

- The health plans selected appropriate SSSGs;
- The FEHBP rates are equivalent to those charged to the SSSGs; and
- The loadings applicable to the FEHBP rates are appropriate and reasonable.

A **loading** is a rate adjustment that participating carriers add to the FEHBP rates to account for additional benefits not included in its basic benefit package.

Medical Loss Ratio Audits

In April 2012, OPM issued a final rule establishing an FEHBP-specific MLR requirement to replace the SSSGs comparison requirement for most community-rated FEHBP carriers.

Medical Loss Ratio is the proportion of health insurance premiums collected by a health insurer that is spent on clinical services and quality improvement. The MLR for each insurer is calculated by dividing the amount of health insurance premiums spent on clinical services and quality improvement by the total amount of health insurance premiums collected. The MLR is important because it requires health insurers to provide consumers with value for their premium payments.

The FEHBP-specific MLR rules are based on the MLR standards established by the Affordable Care Act (ACA). In 2012, community-rated FEHBP carriers could elect to follow the FEHBP-specific MLR requirements instead of the SSSGs requirements. Beginning in 2013, the MLR methodology was required for all community-rated carriers, except those that are state mandated to use traditional community rating. State-mandated traditional community rating carriers continue to be subject to the SSSGs comparison rating methodology, which was amended in 2015 to require only one rather than two SSSGs.

The FEHBP-specific MLR requires carriers to report information related to earned premiums and expenditures in various categories, including reimbursement for clinical services provided to enrollees, activities that improve healthcare quality, and all other non-claims costs. If a carrier fails to meet the FEHBP-specific MLR threshold, it must pay a subsidization penalty to OPM. Since the claims cost is a major factor in the MLR calculation, we are currently focusing our efforts on auditing the FEHBP claims used in the MLR calculation.

The following summaries highlight notable audit findings for community-rated FEHBP carriers audited during this reporting period.

TakeCare Insurance Company, Inc.

Tamuning, Guam
Report Number 1C-JK-00-18-029
April 25, 2019

TakeCare Insurance Company, Inc. (TakeCare Plan) has participated in the FEHBP since 1998, and provides health benefits to FEHBP members on the island of Guam, the commonwealth of the Northern Mariana Islands, and the Republic of Palau. The audit covered contract years 2013 through 2016. During this period,

the FEHBP paid the TakeCare Plan approximately $141 million in premiums.

Lack of controls over the FEHBP MLR process led to penalties and lost investment income due to OPM

We determined that portions of the MLR calculations were not prepared in accordance with the laws and regulations governing the FEHBP and the requirements established by OPM. This resulted in MLR penalty underpayments due to OPM for contract years 2013 through 2016. Additionally, lost investment income (LII) was due on the unpaid penalties through March 31, 2019. LII results from excess withdrawals from the FEHBP trust fund that could have been placed in income producing investments and accounts.

Specifically, we found that the TakeCare Plan:

- Did not have sufficient internal controls over the FEHBP MLR process;
- Did not follow OPM's 2014 Community Rating Guidelines and filed separate MLR forms for plan codes that cover the same area;
- Was not in compliance with OPM's Claims Data Requirements Carriers Letter for contract years 2013 through 2016;
- Included unallowable administrative costs in the incurred claims totals for contract years 2013 through 2016;
- Did not allocate Quality Health Improvement expenses and tax expenses to the FEHBP accurately and appropriately for all contract years;
- Reported unallowable expenses for both the numerator and the denominator of the MLR calculation in contract years 2013 through 2016; and
- Was not in contractual compliance regarding the electronic submission of provider claims.

Blue Care Network of Michigan

Southfield, Michigan
Report Number 1C-LX-00-18-031
June 4, 2019

Blue Care Network of Michigan (Blue Care MI Plan) has participated in the FEHBP since 1984, and provides health benefits to FEHBP members in East and Southeast Michigan. The audit covered contract years 2013 through 2016.

We determined that portions of the MLR calculations were not prepared in accordance with the laws and regulations governing the FEHBP and the requirements established by OPM. This resulted in MLR credit reductions totaling $879,925 for contract years 2013 through 2015. Although we identified issues in contract year 2016, they did not result in a penalty due to OPM or a credit due to the Blue Care MI Plan.

Specifically, we found that the Blue Care MI Plan:

- Included claims for ineligible non-disabled dependents in contract years 2013 through 2016;
- Terminated coverage early for eligible non-disabled dependents in contract years 2013 through 2016;
- Was unable to support its medical incentive pool and bonus amount in contract year 2013;
- Erred in its pharmacy rebates calculation in contract year 2013;
- Used an unsupported pharmacy rebate amount in its contract year 2016 FEHBP MLR submission; and
- Was unable to provide support for the basis of its allocations methods for contract years 2013 through 2016.

Ineffective enrollment controls led to ineligible dependents having claims processed and paid by the health plan.

Experience-Rated Carriers

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. Experience-rated HMOs also fall into this category. The universe of experience-rated plans currently consists of approximately 60 audit sites, some of which include multiple plans. When auditing these plans, our auditors generally focus on three key areas:

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

Blue Cross Blue Shield Service Benefit Plan Audits

The BCBS Association, on behalf of 64 participating plans offered by 38 BCBS companies, has entered into a Government-wide Service Benefit Plan contract with OPM to provide a health benefit plan authorized by the Federal Employees Health Benefits Act of 1959. The BCBS Association delegates authority to participating local BCBS plans throughout the United States to underwrite and process the health benefit claims of its Federal subscribers. Over 60 percent of all FEHBP subscribers are enrolled in BCBS plans.

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

The following are two summaries of recent BCBS audits that are representative of our work.

BlueCross BlueShield of Alabama

Birmingham, Alabama
Report Number 1A-10-09-18-050
July 11, 2019

Our audit of the FEHBP operations at BCBS of Alabama (BCBS of AL) covered health benefit payments and credits, such as refunds and medical drug rebates, from 2013 through March 2018, as well as administrative expense charges from 2013 through 2017. We also reviewed the BCBS of AL's cash management activities and practices related to FEHBP funds from 2013 through March 2018, and the plan's fraud and abuse program activities from January 2018 through June 2018.

We questioned $4,684,247 in medical drug rebates, administrative expense charges, and LII. The BCBS Association and BCBS of AL agreed with all of the questioned amounts.

Specifically, our audit identified the following:

- We questioned $224,411 for medical drug rebates that had not been returned to the FEHBP and

$33,747 for LII on health benefit refunds and recoveries, hospital settlements, and medical drug rebates that were returned untimely to the FEHBP.

- We questioned $3,044,436 for executive compensation overcharges, $722,715 for unallowable expenses, $300,157 for non-recurring cost overcharges, $65,661 for unallowable merger and acquisition costs, $17,145 for ACA fee overcharges, and $275,975 for LII on these questioned charges.
- There were no findings pertaining to the BCBS of AL's cash management activities and practices. Overall, we determined that BCBS of AL handled FEHBP funds in accordance with the contract and applicable laws and regulations.
- There were no findings pertaining to the BCBS of AL's fraud and abuse program activities. We concluded that BCBS of AL is in compliance with the applicable communication and reporting requirements for fraud and abuse cases.
- We verified that BCBS of AL subsequently returned all questioned amounts to the FEHBP.

Pension, Post-Retirement Benefit, and Affordable Care Act Costs for a Sample of BlueCross and/or BlueShield Companies

Washington, D.C.
Report Number 1A-99-00-18-045
August 7, 2019

Our focused audit of the FEHBP operations at a sample of 18 BCBS companies covered pension, post-retirement benefit, and ACA costs that were charged to the FEHBP from 2014 through 2017.

We questioned $1,138,828 in administrative expense overcharges and LII. The BCBS Association and applicable BCBS companies agreed with all of the questioned amounts. As part of our review, we verified that the BCBS companies subsequently returned these questioned amounts to the FEHBP.

Our audit results are summarized as follows:

- We determined that three of the BCBS companies in our sample overcharged the FEHBP $12,250 for pension costs. The questioned LII totaled $596 for these overcharges.
- We determined that one BCBS company in our sample overcharged the FEHBP $178,636 for post-retirement benefit costs. The questioned LII totaled $6,206 for these overcharges.
- We determined that eight of the BCBS companies in our sample overcharged the FEHBP $791,329 for ACA costs. We also determined that another BCBS company returned ACA cost overcharges to the FEHBP during the audit scope, but had not calculated and returned applicable LII to the FEHBP. The questioned LII totaled $72,146 for these exceptions.
- Two BCBS companies self-disclosed additional administrative expense overcharges of $73,007 to the FEHBP which were not related to pension, post-retirement benefit, and ACA costs. The questioned LII totaled $4,658 for these overcharges. We calculated total LII for these overcharges to be $83,606.

Global Audits

Global audits of BCBS plans are cross-cutting reviews of specific issues we determine are likely to cause improper payments. These audits cover all 64 BCBS plans offered by the 38 participating BCBS companies.

We issued one global audit report during the reporting period.

Audit of Coordination of Benefits with Medicare for BlueCross and BlueShield Plans

Global Audit of all BlueCross BlueShield Plans
Report Number 1A-99-00-19-001
September 19, 2019

The audit covered the coordination of health benefit payments (COB) between Medicare and the FEHBP for all BCBS plans from October 1, 2017, through June 30, 2018. Our audit determined that the BCBS Association has implemented corrective action to prevent some COB claim payment errors, resulting in a 73-percent reduction in identified overpayments from our previous COB audit.

However, we still identified $1,355,514 in FEHBP COB overpayments.

Specifically, we found that BCBS plans:

- Incorrectly used a Medicare Payment Disposition Code to override the claim system's automatic deferral of claims, resulting in the improper payments of 1,233 claim lines, totaling $756,612 in FEHBP overcharges;
- Incorrectly paid 79 claim lines due to provider billing errors. These errors resulted in FEHBP overcharges totaling $73,093;
- Did not appropriately defer claims within the BCBS nationwide claims processing system (FEP Express), which should have been deferred for a Medicare COB review. This error resulted in the improper payment of 308 claim lines, totaling $122,428 in FEHBP overcharges;
- Did not retroactively review and/or adjust patients' prior paid claim(s) when a member's Medicare information was added to FEP Express. This error resulted in the improper payment of 451 claim lines, totaling $358,438 in FEHBP overcharges; and
- Incorrectly paid 174 claim lines for non-COB-related errors. In most cases, the errors occurred because the BCBS plans used an incorrect pricing allowance to pay the claims. These errors resulted in the improper payment of $44,943 in FEHBP overcharges.

Various BCBS plans' processing/payment errors resulted in improper claim payments of $1,355,514, representing 2,245 claim lines.

The BCBS Association agreed with all of our audit findings, but had exhausted recovery efforts on $35,651 of the total amount questioned. This leaves $1,319,863 that either has been or remains to be recovered. This audit remains open, pending recovery of the remaining amounts.

Employee Organization Plans

Employee organization plans fall into the category of experience-rated plans. These plans either operate or sponsor participating Federal health benefits plans. 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 of the employee organizations that participate in the FEHBP include: 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 the Special Agents Mutual Benefit Association.

We did not issue any audit reports of 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 previously explained on page 1 of this report, the key difference between the categories stems from how premium rates are calculated.

We did not issue any experience-rated comprehensive medical plan audit reports during this reporting period.

Multi-State Plan Program

The Multi-State Plan (MSP) Program was established by § 1334 of the ACA. This provision directs OPM to contract with private health insurers (called issuers) to offer MSP products in each state and Washington, D.C. OPM negotiates contracts with MSP Program issuers, including rates and benefits, in consultation with states and marketplaces. In addition, OPM monitors the performance of MSP Program issuers and oversees compliance with legal requirements and contractual terms. OPM's Program Development and Support office, formerly the National Healthcare Operations office, has overall responsibility for program administration.

In 2017, the MSP Program universe consisted of approximately 23 state-level issuers covering 22 states. In 2018 and 2019, however, there was only one issuer that participated in the program (Arkansas BCBS). Our audits of the MSP Program assess the issuer's compliance with the provisions of its contract with OPM and applicable Federal laws and regulations.

We did not issue any final reports for MSP audits during this reporting period.

Information Systems Audits

OPM manages a wide portfolio of information systems to help fulfill its mission. OPM systems support agency financial activity, the processing of retirement claims, and multiple Government-wide human resources services such as the USAJOBS website. Private health insurance carriers participating in the FEHBP rely upon information systems to administer health benefits to millions of current and former Federal employees and their dependents. The ever-increasing frequency and sophistication of cyber attacks on both the private and public sector make the implementation and maintenance of mature cybersecurity programs a critical need for OPM and its contractors. Our information technology audits identify potential weaknesses in the auditee's cybersecurity posture and provide tangible strategies to rectify and/or mitigate those weaknesses. The selection of specific audits to conduct each year is based on a risk assessment model that considers various factors, including the size of the health insurance carrier, the sensitivity of the information in the system, the time elapsed since the last audit, and our previous audit results.

Our audit universe encompasses all 47 OPM-owned information systems as well as the 75 information systems used by private sector entities that contract with OPM to process Federal data. We issued four IT system audit reports during the reporting period, which are summarized below.

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

Washington, D.C.
Report Number 4A-CI-00-18-037
April 25, 2019

The Federal Information Technology Acquisition Reform Act (FITARA) grants Chief Information Officers (CIOs) expanded authorities to manage and approve the oversight of IT processes at Federal agencies. Specifically, FITARA outlines the CIO responsibilities related to IT project planning and implementation through governance structures, participating in agency budgeting activities, approving contracts, and personnel decisions.

OPM has taken steps to enable its CIO to function as the head of the agency's IT; however, our audit determined that OPM still is not fully compliant with the requirements of FITARA. We identified the following issues:

- OPM's CIO is not always included in budget discussions around core operating funds involving IT systems for other program offices;
- OPM's CIO is not always included in reprogramming discussions for funds involving IT systems for other program offices;
- OPM's CIO is not properly approving contracts and agreements for OPM's major IT investments; and
- There were instances where the documentation approving OPM's acquisition of IT or IT services contained inaccurate information.

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resource Integration Data Warehouse

Washington, D.C.
Report Number 4A-CI-00-19-006
June 17, 2019

The Enterprise Human Resource Integration Data Warehouse (EHRIDW) is one of the OPM's major IT systems.

Our audit of the IT security controls of the EHRIDW determined that:

- Six of the seven required the EHRIDW Security Assessment and Authorization (Authorization) security documents we reviewed were out of date and/or inaccurate at the time the Authorization was granted.
- The EHRIDW security categorization is consistent with both the Federal Information Processing Standards 199 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, and we agree with the "high" categorization. However, the document was not signed by the current System Owner, Chief Information Security Officer, or Authorizing Official.
- The EHRIDW Privacy Threshold Analysis and Privacy Impact Assessment are out of date and contain information inconsistent with other system documentation.
- The EHRIDW System Security Plan follows the OCIO's template but does not adequately reflect the state of the system at the time of fieldwork.
- An independent security assessment was not conducted on EHRIDW prior to the Authorization being granted.
- Information security continuous monitoring for EHRIDW was conducted in accordance with the agency's quarterly schedule for FY 2018.
- The EHRIDW contingency plan is out of date, inaccurate, and has not been tested annually.
- The EHRIDW Plan of Action and Milestones documentation is not up to date and contains 65 identified weaknesses that are at least a year old and past their scheduled completion dates.
- We evaluated a subset of the system controls outlined in NIST SP 800-53, Revision 4. We determined most of the security controls tested appear to be in compliance. However, we did note several areas for improvement regarding policy and procedures, role-based security training, and vulnerability scanning.

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

Downey, California
Report Number 1C-59-00-19-005
July 23, 2019

Our IT audit focused on the claims processing applications used to adjudicate FEHBP claims for Kaiser Foundation Health Plan, Inc., Northern California and Southern California Regions (Kaiser of CA), as well as the various processes and IT systems used to support these applications. Our audit of Kaiser of CA IT security controls determined that:

- The Kaiser of CA Plan has developed an adequate risk management methodology and creates remediation plans to address weaknesses identified in risk assessments.
- Access controls appear to be appropriately provisioned, enforced, and reviewed.
- System configuration is controlled according to documented policies, procedures, and standards.
- Kaiser of CA has an adequate service continuity process to respond to and recover from unexpected disruptions.
- Kaiser of CA follows a standardized application development and change control process.
- Proper controls have been implemented to protect sensitive data throughout the claims adjudication process.

OPM Cybersecurity Program

In the FY 2019 Senate Appropriations Committee Financial Services and General Government Appropriations Bill Report, S. Rept. 115-281, the Subcommittee

encouraged the OIG to include in its Semiannual Reports to Congress a discussion of: OPM's efforts to improve and address cybersecurity challenges including steps taken to prevent, mitigate, and respond to data breaches involving sensitive personnel records and information; OPM's cybersecurity policies and procedures in place, including policies and procedures relating to IT best practices such as data encryption, multifactor authentication, and continuous monitoring; OPM's oversight of contractors providing IT services; and OPM's compliance with government-wide initiatives to improve cybersecurity.[5] These issues are discussed below.

OPM's efforts to improve and address cybersecurity challenges

OPM has made significant improvements in its technical IT security environment since 2015, including two-factor authentication at the network level, data encryption, incident response, patch management, and an improved network architecture. However, OPM has struggled to implement an IT security governance program to ensure that these controls remain effective.

OPM has defined and communicated a data breach response plan and established a data breach response team. However, OPM does not currently conduct routine exercises to test the plan, which includes requirements for quarterly reviews and annual testing. Failure to test the plan could increase OPM's risk of a major data loss in the event of a security incident.

OPM's cybersecurity policies and procedures

OPM has implemented data encryption on data at rest and in transit for the agency's most sensitive systems. However, multifactor authentication is in place only for authentication to the OPM network. Multifactor authentication for OPM applications has still not been implemented. Enforcing the use of Personal Identity Verification (PIV) authentication to connect to the agency's network is not sufficient, as users or attackers that do gain access to the network can still access OPM applications containing sensitive data with a simple username and password. If PIV authentication were put in place at the application level, an attacker would have extreme difficulty gaining unauthorized access to data without having physical possession of an authorized user's personal identity verification card. OPM has noted that it cannot fully implement multifactor authentication because many of its legacy applications do not support that technology. This situation further demonstrates the importance of OPM's IT Modernization Plan.

OPM has not fully implemented information security continuous monitoring (ISCM), but has developed a strategy that addresses the monitoring of security controls at the organization, business unit, and individual information system level. However, the agency has not successfully implemented several key objectives. OPM has ISCM in place for only 28 of OPM's 47 major systems. Of those 28, only 8 systems were subject to adequate security controls testing and monitoring in compliance with OPM policies, procedures, and submission schedules.

OPM's oversight of contractors providing IT services

OPM requires the same level of security compliance for contractor-operated systems as OPM internal systems with regard to security authorization, continuous monitoring, and disaster recovery plans and testing. OPM also requires contractors to participate in the agency's IT security awareness training before providing access to OPM systems. However, OPM has struggled with monitoring contractors' system access after it has been granted.

5 Financial Services and General Government Appropriations Bill Report, S. Rept. 115-281.

OPM's compliance with Government-wide initiatives to improve cybersecurity

OPM has implemented security tools associated with the Department of Homeland Security's (DHS) Continuous Diagnostics and Mitigation program to automate security of the agency's network, and uses the DHS trusted internet connection initiative to optimize the security of the agency's external network connections.

Internal Audits

Our internal auditing staff focuses on improving the efficiency and effectiveness of OPM operations and their corresponding internal controls. Our auditors are also responsible for conducting or overseeing certain statutorily required audits, including the annual audit of OPM's consolidated financial statements required under the Chief Financial Officers Act of 1990. Our staff also conducts performance audits covering other internal OPM programs and functions. The selection of specific audits to conduct each year is based on a risk assessment model that considers various factors, including the size of the program, the time elapsed since the last audit, and our previous audit results.

Fiscal Year 2018 Improper Payments Reporting Washington, D.C.

Report Number 4A-CF-00-19-012
June 3, 2019

The OIG annually audits OPM's reporting of improper payments to assess compliance with the Improper Payments Information Act of 2002 (IPIA), as amended by the Improper Payments Elimination and Recovery Act of 2010 (IPERA) and the Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), as well as implementation of Office of Management and Budget (OMB) guidance. Compliance with IPERA requires that agencies do the following:

- Publish an Agency Financial Report (AFR) or Performance and Accountability Report (PAR) for the most recent fiscal year (FY)and post that report and any accompanying materials required by OMB on the agency website;
- Conduct a program-specific risk assessment for each program or activity that conforms with 31 United States Code (U.S.C.) § 3321 (if required);
- Publish improper payment estimates for all programs and activities identified as susceptible to significant improper payments under its risk assessment (if required);
- Publish programmatic corrective action plans in the AFR or PAR (if required);
- Publish and meet annual reduction targets for each program assessed to be at risk and estimated for improper payments (if required and applicable); and
- Report a gross improper payment rate of less than 10 percent for each program and activity for which an improper payment estimate was obtained and published in the AFR or PAR.

Our audit found that OPM complied with IPERA's six requirements for FY 2018. We further determined that OPM complied with additional reporting requirements imposed by IPERIA, which include the use of the Do Not Pay portal and obtaining approval for both the improper payment rates and reduction targets. In addition, we identified one area where OPM can improve its internal controls over improper payments reporting. Specifically, OPM's Disability Earnings Match improper payments amount was underreported by $132,659.

Special Audits

In addition to health insurance and retirement programs, OPM administers various other benefit programs for Federal employees, which include:

- 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 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 and annuitants are properly handled and disbursed to charities according to the designations of contributing employees, and audits of Tribal enrollments into the FEHBP.

BENEFEDS as Administered by Long Term Care Partners, LLC, for Contract Years 2014 through 2016

Portsmouth, New Hampshire
Report Number 1G-LT-00-18-040
September 11, 2019

BENEFEDS consists of the system and business structures necessary to administer the enrollment and/or premium administration functions associated with multiple voluntary Federal benefits, including FEDVIP, FSAFEDS, and FLTCIP. It includes an online benefit management portal allowing eligible users to access information about and make changes to their benefits in the above mentioned programs.

There are four major components to BENEFEDS:

- An enrollment website (www.benefeds.com);
- Data transmission to and from the carriers;
- A premium administration system; and
- A customer service system.

Long Term Care Partners, LLC (LTCP), a wholly owned subsidiary of John Hancock Life & Health Insurance Company, was created in 2002 to administer the FLTCIP. In 2006, the LTCP assumed the responsibility for the development, maintenance, and administration of BENEFEDS necessary to facilitate the administrative functions of the FEDVIP and the FSAFEDS.

Compliance with the laws, regulations, and contractual requirements applicable to BENEFEDS is the responsibility of the LTCP's management. In addition, management of the LTCP is responsible for establishing and maintaining a system of internal controls.

The main objective of the audit was to determine whether costs charged to BENEFEDS and services provided to its users were in accordance with terms of the OPM contract and applicable Federal regulations. Our audit consisted of a review of the LTCP's administrative expenses, cash management, coordination of benefits, enrollment eligibility, fraud and abuse program, and

performance standards for BENEFEDS operations during contract years 2014 through 2016.

The results of our audit determined that the LTCP needs to work with OPM to strengthen procedures and controls related to dependent eligibility and fraud and abuse for BENEFEDS operations. Specifically, our audit identified the following deficiencies that require corrective action:

- OPM and the LTCP have insufficient policies and procedures in place to prevent ineligible dependents from participating in the FEDVIP. In fact, FEDVIP enrollees simply self-certify family members with no requirement for the carriers or BENEFEDS to verify dependent eligibility.
- The LTCP does not have a vigorous fraud and abuse program in place to assess vulnerabilities and help detect and eliminate fraud and abuse for BENEFEDS operations.

No other exceptions were identified from our reviews of administrative expenses, cash management, coordination of benefits, and performance standards.

BENEFEDS self-certification process allows ineligible dependents to enroll in the FEDVIP.

Federal Long Term Care Insurance Program Operations as Administered by Long Term Care Partners, LLC for Contract Years 2013 through 2016

Portsmouth, New Hampshire
Report Number 1G-LT-00-19-003
July 17, 2019

The FLTCIP was established by the Long Term Care Security Act (Public Law 106-265), which was signed on September 19, 2000. The Act directed OPM to develop and administer a long-term care insurance program for Federal employees and annuitants, current and retired members of the uniformed services, and their qualified relatives.

OPM's Federal Employee Insurance Operations, Life and Ancillary Benefits group has overall responsibility for administering the FLTCIP, including the publication of program regulations and agency guidelines. OPM contracts with the LTCP to administer the FLTCIP. The LTCP's responsibilities under the contract are carried out at its office in Portsmouth, New Hampshire. Section I.10 of the contract includes a provision that allows for audits of the LTCP's operations (Inspection of Services-Fixed Price). The LTCP entered into a new contract with OPM for the administration of the FLTCIP on May 1, 2016.

The main objective of the audit was to determine whether costs charged to the FLTCIP and services provided to FLTCIP participants were in accordance with the terms of the contract and the applicable Federal regulations. Our audit consisted of a review of administrative expenses, cash management, claims processing, and performance guarantees as they related to the FLTCIP for contract years 2013 through 2016 (through the close out of the contract).

The results of our audit showed that the LTCP properly charged all costs to the FLTCIP and provided services to the FLTCIP participants in accordance with the contract. Consequently, our audit disclosed no findings pertaining to our reviews of administrative expenses, cash management, claims processing, and performance guarantees for contract years 2013 through 2016 and no corrective action was necessary.

The results of our audit showed that the LTCP properly charged all costs to the FLTCIP

Investigative Activities

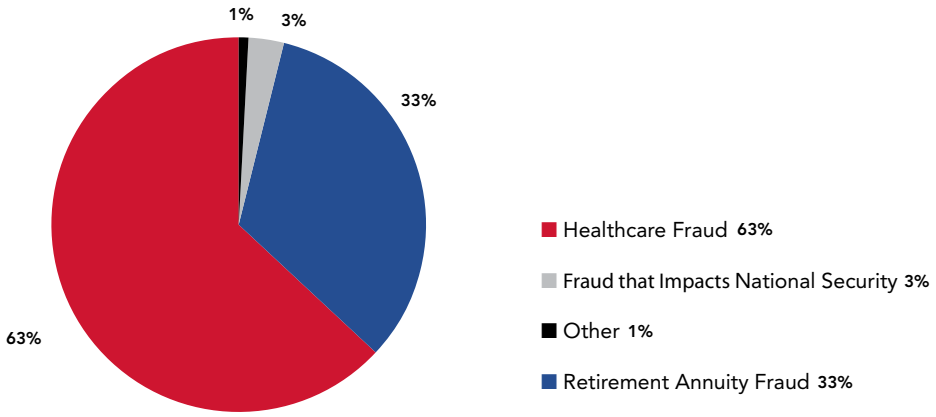
The Office of Investigations prioritizes our investigative resources to protect current and retired Federal employees and their family members from patient harm and to protect OPM's financial and programmatic integrity. OPM-administered trust funds, from which benefits are paid under the Civil Service Retirement System (CSRS), the Federal Employees Retirement System (FERS), FEHBP, and FEGLI, amount to over $1 trillion. These programs cover over 8 million current and retired Federal civilian employees and eligible family members, and disburse over $140 billion in benefits annually.

We conduct criminal, civil, and administrative investigations of fraud, waste, abuse, and mismanagement against OPM programs and operations to protect the 8 million current and retired Federal civilian employees and eligible family members who participate in the FEHBP and/or Retirement Program and to safeguard the $1 trillion in trust funds that pay OPM program benefits. Our investigations often lead to criminal convictions, civil and criminal recoveries, and administrative corrective actions such as debarment from participation in other Federal programs. We also actively coordinate with the U.S. Department of Justice (DOJ) and other Federal, State, and local law enforcement authorities on cases as part of our mission to protect Federal employees, annuitants, and their families. The chart below shows the OIG's Enforcement Actions by Case Type.

We are a partner in the Nation's ongoing fight against the opioid epidemic. Our investigations target bad actors who propagate the crisis, exploit those seeking treatment for addiction and related services, and harm Federal employees, retirees, and the FEHBP.

Our investigations prevent, reduce, and stop improper payments and protect the integrity of OPM programs, including the FEHBP and Retirement Programs. This ultimately protects taxpayer dollars. As part of our alignment with the President's Management Agenda goal to reduce improper payments, we pursue investigations and proactive work that returns money to the OPM trust

ENFORCEMENT ACTIONS BY CASE TYPE



funds through civil recoveries and criminal restitutions. Our investigations and proactive work also protects the safety of FEHBP subscribers. We also participate in cases that return funds to the Government through administrative remedies, such as contractual payment offsets and credits. In this reporting period, we participated in cases that returned over $1.2 billion to the General Fund of the U.S. Treasury. Our investigations also led to 56 indictments and informations, 42 arrests, 56 convictions, and over $20 million in recoveries to OPM-administered trust funds.

Below we provide an overview of our investigative priorities, as well as observed trends in fraud, waste, and abuse. We also provide case summaries representative of the Office of Investigation's diligent work to protect OPM, its programs, and the Federal employees and retirees and family members who rely on those programs. To the extent that pending criminal matters are discussed herein and unless otherwise explicitly stated, the crimes and charges are alleged and all defendants and parties are presumed innocent unless proven guilty in a court of law.

Our investigations led to 56 indictments and informations, 42 arrests, 56 convictions, and the recovery to OPM of over $20 million

The Opioid Epidemic

For the first time since 1990, overdose deaths in the United States are in decline. Progress against the opioid crisis is happening. Still, there remains a long way to go: on average, every day still brings the death of 130 Americans from opioid overdose. In 2018, more than 68,000 Americans died from overdose. Comorbid diseases associated with the crisis such as endocarditis, hepatitis, and others increase long-term health-care costs and contribute to even more deaths. Criminals and bad actors participate in the diversion or improper prescription of opioids into the hands of those addicted and use fraudulent schemes to exploit those seeking drug abuse and addiction treatment. Fraud by marketers, drug makers, and distributors who contribute to the crisis for their gain perpetuates the nationwide scourge of opioid and drug abuse.

The OIG continues to fight the opioid crisis and its effects on Federal employees, retirees, and their dependents. Our investigative priorities address the crisis at all levels, from bad doctors and prescribers to unethical pharmaceutical companies whose tactics make Americans less safe, healthy, and well. These efforts include participating in National Takedown Week and other joint ventures with law enforcement partners on the local and national level, as well as working with private FEHBP health insurance carriers and their opioid abuse prevention strategies. The SUPPORT Act, and the enacted Eliminating Kickbacks in Recovery Act of 2018, allows us to pursue unethical providers, including patient brokers, those accepting or providing kickbacks to treatment centers, and others who would unduly profit off the suffering of both those in recovery and their families.

In his September 6, 2019, remarks during Opioid Crisis Awareness Week, President Donald J. Trump discussed some of the Administration's initiatives to abate the crisis, including "approaching addiction as a treatable disease." OPM has worked with FEHBP carriers to increase treatment availability and promote insurance carriers using effective treatments such as medically assisted therapy. The OIG, through its investigations, has protected those in recovery from fraud schemes that would exploit and harm patients. In our Semiannual Report for October 1, 2018, through March 31, 2019, we detailed two of these types of fraud schemes in recovery settings. We continue to investigate cases across the entire web of addiction—from drug makers to pill mills

to treatment centers—as part of our investigative focuson patient harm.[6]

The following case summaries highlight our efforts in fighting the opioid epidemic as it affects the FEHBP.

Opioid Manufacturer

- **Insys Pharmaceuticals Executives Prosecuted Under RICO Act.** In May 2019, our joint law enforcement investigation into Insys Pharmaceuticals, the maker of fentanyl-based pain patch Subsys, ended in five convictions, including convictions under the Racketeer Influenced and Corrupt Organizations (RICO) Act. The U.S. Attorney's Office for Massachusetts called the case the first successful prosecution of an opioid manufacturing company.

  Insys took actions that were criminal, callous, and dangerous. Its employees pushed doctors to prescribe Subsys beyond medically recognized uses in exchange for inducements; falsified and misrepresented information for prior authorizations via a sham "reimbursement center;" and encouraged the titration of prescriptions to higher doses that increased the risk of serious patient harm, including opioid addiction and death.

  Testimony at trial from former employees and executives detailed incidents of bribery and inappropriate relationships between doctors and executives. At the Insys reimbursement center, employees of the company pretended to be or misrepresented themselves as medical providers when contacting insurance companies to get prior authorization for Subsys prescriptions. Often, the patients represented by the reimbursement center had no history of cancer-related pain, the only U.S. Food and Drug Administration-approved use of Subsys. Staff bonuses tied to titration schemes pressured employees to put patients at risk for financial benefit and supported an avaricious company culture.

  From April 2012 to September 2016, the FEHBP paid over $17 million for more than 2,000 claims related to Insys. Our investigators conducted document reviews, interviewed patients, and participated in the arrests, criminal proceedings, and other essential law enforcement activities during the 5-year investigation and subsequent trial. In addition to the convictions, several individuals pled guilty to crimes including healthcare and wire fraud, and the U.S. District Court for the District of Massachusetts approved a settlement including global restitution of $2 million in fines, $28 million in forfeiture, and $195 million to settle allegations related to violations of the False Claims Act. The FEHBP will recover $3.7 million.

Pill Mill

- **Maryland Fentanyl-Dealing Providers Exchanged Sexual Favors for Prescriptions.** In July 2019, a provider pled guilty to conspiracy to distribute and dispense a controlled substance after an investigation into off-label prescriptions and kickbacks related to fentanyl-based medications, including Subsys, and other opioids. The FEHBP paid this provider almost $2.1 million for Schedule II prescriptions.[7]

  Interviews revealed providers issued prescriptions without legitimate medical need and beyond the bounds of acceptable medical practice. One provider also admitted to writing prescriptions for patients in exchange for sexual favors.

6 A pill mill is an operation in which a healthcare provider, facility, or pharmacy prescribes and/or dispenses drugs without a legitimate medical purpose.

7 Schedule II prescription medications have a high potential for abuse which may lead to severe psychological or physical dependence.

Treatment

- **Doctor Receives 3-Year Prison Sentence in $3 Million Pass-Through Billing Scheme.** A behavioral health provider group that exploited patients seeking treatment for drug and alcohol addiction engaged in a variety of healthcare fraud schemes. Between April 2019 and September 2019, our investigation led to the indictment and arrest of more than 10 individuals. Several subjects, including two doctors and the facility owner, pled guilty to healthcare fraud. On September 20, 2019, one doctor was sentenced to 3 years in prison and ordered to pay $2.48 million in restitution, of which $314,593 will be returned in a lump sum to the FEHBP.

  The provider group admitted ineligible beneficiaries, provided substandard care, and illegally boarded patients in company-owned housing in order to maximize the fraud. According to information presented at trial, these company-owned houses became places where drug use continued and there were inappropriate sexual relationships between patients and staff. As part of this scheme, the behavioral health provider created a kickback scheme to send unnecessary urinalysis to laboratories that billed at exorbitant rates and paid kickbacks to the behavioral health provider. These crimes ultimately cost the FEHBP over $3.1 million.

- **Rural Hospital and Substance Abuse Treatment Pass-Through Scheme Broken Up.** A rural hospital pass-through billing fraud scheme generated more than $10 million in ill-gotten gains from the FEHBP as part of a kickback arrangement involving urinalysis testing and several substance abuse treatment facilities in Florida. In July 2019, one target pled guilty in the U.S. District Court for the Middle District of Florida to conspiracy to commit money laundering. As part of the plea agreement, the defendant will forfeit all property traceable to the offense.

Ineligible Family Members

Ineligible family members receiving FEHBP benefits contribute to higher premiums, higher program costs, and wasted taxpayer dollars. These benefits are often propagated through deliberate fraud by FEHBP enrollees and preserved by program vulnerabilities or oversights that allow fraudulent improper payments. Federal agencies that do not verify employees' documentation as required, or erroneously certify information to OPM, are responsible for fraud going undetected before ineligible family members are enrolled. Once ineligible family members are enrolled, it is harder to detect, investigate, and prosecute the fraud.

In Carrier Letter 2014-11, OPM stated, "[h]ealth insurance industry standards indicate that up to 10 percent of family members are ineligible for coverage[8]. If this is also determined to be true for the FEHB Program, we will carefully analyze the findings, impacts and appropriate corrective actions to be taken." According to a January 23, 2018, rule change OPM published in the Federal Register (FR) 83 3059, anecdotal evidence suggests 1 to 3 percent of spouses and 4 to 12 percent of children are ineligible for coverage in private-sector health insurance carriers. OPM does not have a current estimate of the number of ineligible family members in the FEHBP. Applying the industry estimates published in 83 FR 3059 to the FEHBP, the program prospectively loses between $256 million and $3 billion annually due to ineligible dependents.

During the annual Open Enrollment season, or in conjunction with certain Qualifying Life Events, Federal employees and annuitants can add and remove eligible family members from their FEHBP health insurance. For

8 Carrier Letters are defined as sub regulatory guidance within the FEHBP, primarily issued by the OPM Healthcare and Insurance program office to provide more detailed guidance and definitions for FEHBP-related laws, regulations, and contractual language.

employees enrolled in FEHBP with a Self Plus One or Self and Family enrollment type, adding members may not even require verification that the new member is eligible, especially if employees have access to self-service human resource portals. While this is convenient for Federal employees, it is also a program vulnerability. Divorce is another cause of substantial ineligible family member fraud. When a Federal employee is ordered by the courts to maintain health coverage for an ex-spouse, some keep their ex-spouse enrolled under the FEHBP despite the ex-spouse being ineligible. The FEHBP suffers a loss of premium and administrative expenses and additional losses from claims paid on behalf of the ineligible ex-spouse.

The OIG currently investigates cases of ineligible family members when notified by FEHBP carriers, employing Federal agencies, and/or hotline tips or other anonymous reports, as well as when cases develop from our proactive work. We have successfully brought cases where ineligible family members cost thousands in fraudulent claims, but we have also encountered obstacles that have stymied our investigations, specifically program weaknesses in the way OPM manages and audits the enrollment of family members. For example, a physician certified a dependent child who turned 26 as being "incapable of self-support" based on a non-disabling sports injury. The dependent used their FEHBP insurance while undergoing costly substance abuse treatment. Even after our investigation, OPM was unable to remove the child from the FEHBP.

While the OIG has provided recommendations to OPM to reduce program vulnerabilities with the enrollment and verification process, these types of fraud will persist until those recommendations or similar solutions are enacted.

Obstacles have stymied our investigations, specifically program weaknesses in the way OPM manages and audits the enrollment of family members.

The following case summaries highlight investigative cases related to ineligible family members added to the FEHBP that were investigated or resolved during the reporting period.

- **Bureau of Prisons Employee Adds Lawyer and Four Children as Ineligible Family Members.** A Bureau of Prisons employee who added a lawyer unrelated to her and the lawyer's four children to an FEHBP health plan was indicted for making false statements relating to healthcare matters, as well as aiding and abetting the same. The employee and another individual pled guilty in April 2019 and were sentenced to 3 years of probation and restitution of the $12,316 that the FEHBP paid for services provided to the ineligible family members.
- **FEHBP Member Alters Divorce Records to Enroll Ineligible Girlfriend.** An FEHBP member and his current spouse had divorced and then later remarried. Sometime after the remarriage, the FEHBP member and his wife no longer lived together as a married couple (despite still being legally married), and the member never removed his wife from the FEHBP. However, in an attempt to add his current girlfriend to the FEHBP, the member altered his previously submitted divorce records from before his remarriage to show he purportedly divorced his spouse in January 2017. In June 2019, the member pled guilty in the U.S. District Court for the Northern District of Alabama to making false statements.
- **Child's Death Reveals $900,000 of Ineligible Dependent Fraud.** The unfortunate death of a child

led to our discovery of seven ineligible family members enrolled in the FEHBP by their grandmother, who lived in a different state and had enrolled them during Open Enrollment through a self-service portal. The FEHBP paid $937,875, including $854,504 for two facility claims for the deceased child. The alleged fraud involved in enrolling the grandchildren was declined for prosecution. Because the family members were eligible for Medicaid, we were able to obtain reimbursement from that program, and thus returned $937,875 to the FEHBP in an administrative recovery.

Timely Notification to the OIG of OPM Data Risks and Integrity Investigation of Senior OCIO Official

In July 2018, the OIG investigated allegations another U.S. Government agency had conducted unauthorized penetration testing of multiple OPM IT systems after discovering a vulnerability that could have allowed for unauthorized access to some security-related personnel information. In the course of that investigation, we found the OPM OCIO did not follow its guidelines for notifying the OIG of such vulnerabilities and that a senior-level OPM OCIO employee made false statements to our investigators.

No evidence indicated that OPM systems were compromised beyond the unauthorized alleged testing by the other U.S. Government agency, and further no evidence indicated data related to the involved IT systems were downloaded or manipulated.

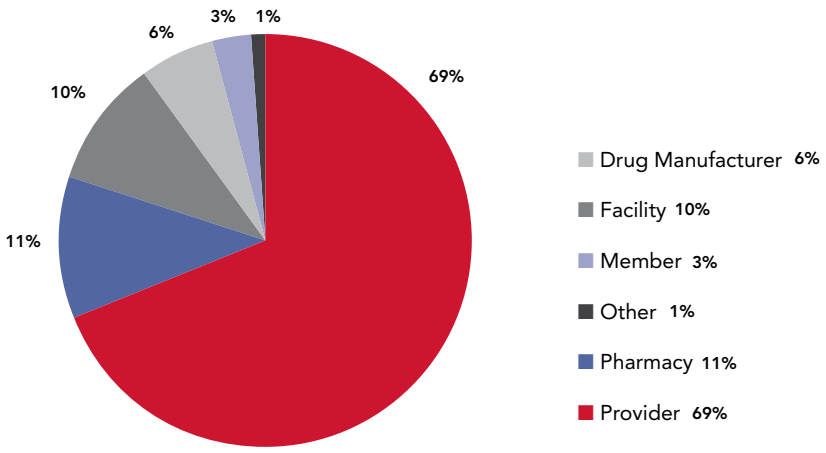
The OIG was not notified of this potential IT security issue by OPM. Instead, the agency alleged to have conducted the unauthorized testing sent reports to the OIG that detailed the vulnerability findings. We reviewed materials from that agency and subsequently received requests from the National Background Investigations Bureau (NBIB) and the OPM OCIO to pursue criminal charges because of the testing. In a discussion with the DOJ's Computer Crime and Intellectual Property Section and Criminal Division Cybersecurity Unit, it was determined that it was unlikely that 18 U.S.C. § 1030, the Computer Fraud and Abuse Act, was violated.

The risk of OPM's failure to notify the OIG of IT system-impacting events is a serious matter. We found that the OPM OCIO did not follow its standard operating procedures for cybersecurity or personally identifiable information-impacting events because it failed to report the issue to the OIG. If the OCIO and the agency had followed its standard operating procedure, the OIG would have been notified much quicker. In the event of a breach or vulnerability that required urgent action, we would have been better positioned to protect the agency and its program integrity.

In addition to OPM's failure to follow its standard operating procedures, including notifying the OIG of the issue, a senior member of the OCIO allegedly made false statements to the Office of Investigations during our investigation. On January 29, 2019, the U.S. Attorney's Office declined to pursue charges for the senior official in lieu of the agency addressing the matter through administrative means.

The final program coordination for this matter concluded in July 2019 when the OIG submitted its report to both the OCIO program office and the agency to take any further necessary action.

CASE SUB-TYPES



Healthcare Fraud in OPM-Adminstered Federal Insurance Programs

The substantial cost of healthcare fraud harms the FEHBP and those who rely on its coverage. The chart above describe our investigative FEHBP case sub-types.

We investigate allegations of fraud, waste, and abuse in the FEHBP, FEDVIP, and other OPM-administered Federal insurance programs. Our cases often involve patient harm, services not rendered, pass-through billing schemes, and other complex healthcare frauds and conspiracies. We pursue these matters to protect Federal employees, retirees and their family members, and to detect and prevent improper payments within the FEHBP universe of over 200 health plans providing insurance coverage for more than 8 million lives.

The Office of Investigations combats an expanding, evolving, and intelligent healthcare crimes ecosystem. Common frauds such as services not rendered, unbundling (billing for multiple codes for a group of procedures that are covered in a single global billing code), and illegal inducements engage with compounding pharmacies, telemedicine, and other novel areas of the healthcare system to create new trends and areas for fraudulent and improper payments.

Our investigations lead to fines, imprisonment, and exclusion from participation in Federal healthcare programs for those whose actions harm FEHBP enrollees or the program. We work in partnership with the DOJ, FBI, and other Federal, State, and local law enforcement partners as part of our nationwide enforcement activities. In addition, we facilitate a Carrier Task Force that brings together FEHBP carriers, representatives of OPM Healthcare and Insurance office, the OIG, and others. The Carrier Task Force provides leads, shares information on emerging trends in healthcare fraud, and sources information to protect the FEHBP. We also participate in the Healthcare Fraud Prevention Partnership.

However, the OIG faces challenges to its investigative operations because of two statutory exclusions. First, because of our exclusion from the Healthcare Fraud and Abuse Control Program (HCFAC), the OIG does not receive a portion of fines and penalties like our law enforcement partners. This rations our investment into and acquisition of investigative technologies and resources. Second, OPM is excluded from using the Anti-Kickback Statute in our investigations, which has prevented prosecutions and the recovery of fraudulently obtained OPM funds.[9]

9 42 U.S.C. §13209-7b(b)

In our previous Semiannual Report for October 1, 2018, to March 31, 2019, we discussed how a novel use of the Travel Act allowed us to investigate cases in conjunction with local anti-kickback and anti-bribery statutes. However, the utility of this tactic is limited. Our exclusion from HCFAC and the Anti-Kickback Statute continues to be a barrier to the Office of Investigations maximizing its financial protection of OPM programs.

The following case summaries highlight our efforts in fighting healthcare fraud as it affects the FEHBP.

- **False Billing Scheme Leads to 5-Year Jail Sentence, $2.4 Million in Restitution.** A Texas provider who pled guilty to making false statements related to healthcare matters was sentenced to 5 years of imprisonment and three years of supervised release related to allegations that the provider allowed an associate to use his provider number and misrepresented the services provided. From the $2.4 million in restitution ordered by the court, the FEHBP will recover its entire damages of $185,405.
- **Fleeing Suspect in $1.1 Million Healthcare Fraud Scheme Apprehended.** In June 2019, we arrested a provider when they appeared to make plans to flee the country after the execution of a search warrant related to alleged healthcare fraud. Another individual related to the scheme previously fled the country.

  The scheme included billing for services not rendered, altering medical records to obscure fraud, and operating a pass-through billing scheme using another entity's provider and tax information. Ultimately, it cost the FEHBP $1.1 million. A criminal complaint for making false statements was filed in the U.S. District Court for the Northern District of Illinois against the subject.

Retirement Benefit Fraud

Fraud committed against CSRS and FERS threatens the integrity of Federal retirement programs. In the worst cases, it stops Federal retirees or their surviving annuitants from receiving essential benefits. We work closely with the new Fraud Branch of OPM Retirement Services, and its addition to the Retirement Services program office has helped us develop leads and investigate fraud in the retirement programs.

Cases of identity theft, whether by strangers or family members, are often at the center of these retirement fraud cases. We commonly investigate forged signatures on Address Verification Letters and other documents used by OPM to verify the status of annuitants. These crimes can be particularly damaging to program integrity because cases may not reach the Office of Investigations until the fraud has been ongoing for years and cost hundreds of thousands of dollars.

Any time an annuitant's identity is compromised, payments from retirement programs become vulnerable to theft and risk potential harm to retirees. As an example, theft and diversion of funds can lead to a lack of appropriate elder care and elder abuse. We investigate cases of identity theft when subjects divert retirement program monies from the rightful recipient, whether through wire fraud and/or unauthorized changes to the bank account where the retirement annuity is electronically deposited. This type of fraud can have a significant impact, especially for single or fixed-income seniors, and we aggressively investigate referrals of this nature.

In our Semiannual Report for October 1, 2018, through March 31, 2019, we detailed a disturbing case ("Starved Annuitant's Caretaker Arrested for Stealing Annuity") that highlights a concerning trend in retirement program investigations: elder abuse. Elder abuse cases often come to the attention of the Office of Investigations due to the

misuse of funds intended for the Federal retiree or their survivor annuitant, but which ends up lining the pockets of those entrusted with their care.

Our investigative resources are also able to help annuitants restore their rightful payments, for example, during this reporting period, we received a referral regarding possible fraud after an alleged annuitant contacted OPM's Retirement Services more than 5 years after the annuity was suspended for payment. Our investigation led us to a nonverbal retiree living at an airport hotel for 10 years and who was owed more than $230,000 by OPM. Our criminal investigator interviewed the annuitant—communicating by writing notes—and was able to verify the retiree's identity. Retirement Services has since restored her annuity.

We work with the DOJ's Elder Justice Initiative resources on applicable cases involving the abuse of Federal annuitants. As the Federal workforce ages and more retirees and annuitants require long-term care, we expect retirement fraud to proliferate, and we will continue to work diligently to protect retired civil servants and their families.

The following case summaries highlight our efforts in fighting fraud that affects the Federal retirement programs.

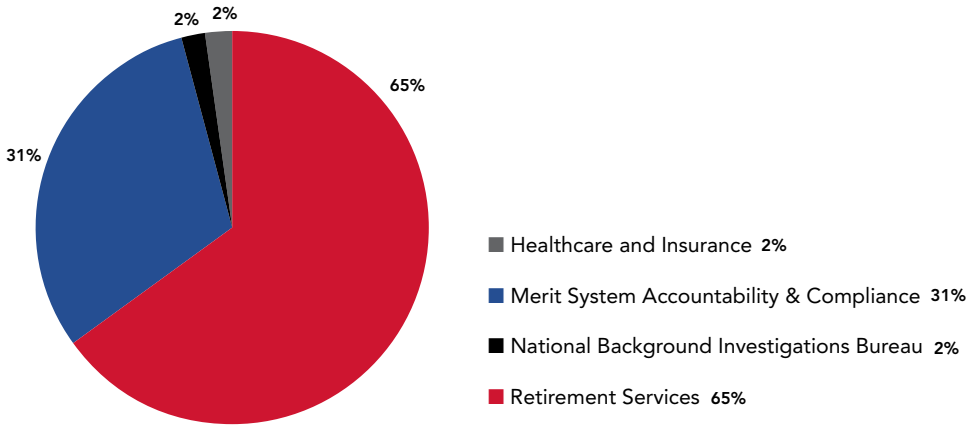
- **Annuitant's Daughter Pleads Guilty to Stealing Annuity for 11 Years.** In June 2019, the daughter of a CSRS annuitant pled guilty in California to the theft of Government property after using $268,369 in funds paid between her parent's death in January 2002 and when the fraud was discovered in January 2013. In addition, OPM paid $88,811 in FEHBP premiums. Some funds were recovered through the Department of the Treasury's reclamation process, but the loss to the Government totaled $352,568.
- **$326,000 Stolen in 24-Year Unreported Annuitant Death.** In May 2018, we received a referral from Retirement Services regarding the unreported April 1993 death of an annuitant. OPM deposited payments through October 2017, resulting in an overpayment of $326,091. The annuitant's daughter offered to repay the debt at $100 per month, but in an interview, she admitted to knowing the money was not rightfully hers and to forging her father's signature on two OPM forms after his death. The daughter was charged in the U.S. District Court for the District of Maryland with theft of Government property. In August 2019, she pled guilty and was sentenced to 36 months of probation, 18 months of home detention, and restitution in the remaining amount of $325,191.
- **Annuitant's Son Indicted for $400,000 Theft of Government Property.** From January 2009 through May 2018, Retirement Services paid $400,491 to the account of a deceased CSRS annuitant. Our investigation discovered the annuitant's son used the money for his gain. In July 2018, OPM recovered $25,678 through the Department of the Treasury's reclamation process. In August 2019, the son was indicted in the U.S. District Court for the District of Maryland for theft of Government property.

Improper Payments in the FEHBP and Retirement Programs

All improper payments are the result of program weaknesses or fraud. In Fiscal Year 2018, OPM reported the FEHBP and Retirement Programs combined to exceed $355.5 million in improper payments.

In the FEHBP and other insurance programs, the OIG's work on improper payments is primarily addressed by the Office of Audits. However, the Office of Investigations does pursue cases where alleged crimes resulted in improper payments. In addition, the Office of Investigations works

PROACTIVE ADMINISTRATIVE RECOVERY CASES



with contracted FEHBP health carriers to return identified improper payments administratively to OPM trust funds through a mutual carrier and provider settlement agreements, as well as through future payment offsets for services rendered by network providers to FEHBP subscribers.

The Office of Investigations also uses its Investigative Support Operations (ISO) group to conduct proactive searches and investigations to uncover improper payments. In particular, we have been successful in identifying retirement cases where program vulnerabilities, weak controls, or other circumstances allowed years, or even more than a decade, of improper payments. We report these cases to Retirement Services for action, and OPM is sometimes able to recover these funds through reclamation processes. In this semiannual reporting period, our proactive cases recovered more than $4.9 million across 55 administrative recoveries and actions.[10] The chart above highlights the OIG's proactive efforts to identify improper payments within OPM programs.

The following case summaries highlight our efforts in fighting improper payments throughout OPM programs.

FEHBP Improper Payments

- **Provider Bills Fraudulent Services to Spouse for $200,000 in Improper Payments.** A provider billed excessive services to a single FEHBP member. Our investigation uncovered that the FEHBP member was the spouse of the provider. In interviews with our investigators, the provider admitted all the services submitted for his spouse were fraudulent. The FEHBP paid $247,195 related to this improper payments fraud scheme. In April 2019, a grand jury indicted the provider in the U.S. District Court for the Eastern District of California.
- **New York Enrollee's Improper Payments to Self Leads to 27 Months in Jail.** An FEHBP member submitted fraudulent claims for services from a nonparticipating provider in order to generate payments to himself. Over the course of the improper payments scheme, the FEHBP loss was $207,506. In March 2019, the member pled guilty in the U.S. District Court for the Southern District of New York to one count of healthcare fraud. The enrollee was sentenced in June 2019 to 27 months of incarceration, 3 years of supervised release, and $502,980 in restitution. Of that, $207,506 will be returned to the FEHBP.

10 This monetary amount only includes recoveries posted by OPM. Because our ISO discovers and allows for the stoppage of improper payments that would continue indefinitely, the recoveries are only part of the Office of Investigation's improper payment results.

- **Chicago Specialty Pharmacy Returns $1.6 million to the FEHBP**. In July 2019, we received a referral from an FEHBP carrier alleging a Chicago-based specialty pharmacy had suspicious billing patterns and potential misuses of the procedural code for the injection of the drug Firazyr. The improper payments primarily went to one FEHBP enrollee. The FEHBP carrier indicated that the provider was willing to return a portion of the identified $6.3 million in improper payments. After a review and discussion, the carrier amended the total loss downward based on the provider argument that, although they were relied upon to manage the amount of doses given to the patient, they were also supplying the medication based the medical orders. As a result, the OIG helped facilitate a carrier and provider agreement to return $1.6 million to the FEHBP.

Of OPM OIG active healthcare fraud cases, 71 percent are categorized as improper payments.

Retirement Improper Payments

- **$102,000 Recovered from Proactive Discovery.** Via our ISO's Patient Discharge Code project, we identified a retired annuitant whose account continued to receive payments for 5 years after the annuitant's April 2014 death. In total, the annuitant received $103,570 in post-death retirement payments, in addition to $41,708 in FEHBP premiums. In April 2019, the Office of the Chief Financial Officer (OCFO) posted a recovery of $102,098 through the Department of the Treasury's reclamation process.
- **$72,000 Annuity, $27,000 in FEHBP Premiums Recovered.** We proactively identified the obituary and death record for a survivor annuitant whose January 2016 death went unreported to OPM. The survivor annuitant's account had received annuity payments until April 2019, with the improper payments totaling $72,340 from the retirement trust fund and $27,799 in FEHBP premiums. ISO notified OPM's Retirement Services of the death. In July 2019, the OPM OCFO posted a recovery of the entire amount of the post-death annuity payments.
- **Proactive Analysis Enables Recovery of $70,000 in Improper Payments.** In September 2017, an annuitant receiving both a retirement annuity and a survivor annuity died, but their death was never reported to OPM. Retirement Services continued to pay the annuities until February 2019. The post-death retirement annuity totaled $36,573, the post-death survivor annuity totaled $20,134, and FEHBP premiums totaled $13,226. OPM ultimately paid $69,974 in improper payments after the annuitant's death. Through the Department of the Treasury's reclamation process, the agency recovered the entire amount.

Impact to National Security

The Office of Investigations provides external oversight to NBIB, which conducts background investigations of Federal job applicants, employees, members of the armed services, and contractor personnel for suitability and security purposes. Unsuitable persons gaining employment or being granted a security clearance due to fraudulent, falsified, incomplete, or incorrect background investigations creates vulnerabilities within the Federal workforce and is a risk to government operations and national security.

Most often, the Office of Investigations pursues allegations of falsified reports of background investigations. These reports are commonly the basis for suitability determinations for employment and security

clearances, including Secret and Top Secret clearances. Falsifications can require the reinvestigation and re-adjudication of background investigations at substantial cost to the Government. However, any fraud, waste, abuse, or misconduct by NBIB background investigators is concerning and undermines the integrity of the background investigation process.

The following case summaries highlight our investigations into wrongdoing by background investigators and the falsification of reports of investigation.

Criminal Activities by NBIB Background Investigators

- **NBIB Background Investigator Sentenced to 25 Years in Prison for Possession of Child Pornography.** In July 2019, an NBIB background investigator pled no contest to video voyeurism, lewd and lascivious molestation, promotion of child pornography, and 25 counts of possession of child pornography. The Seventh Judicial Circuit Court of Florida sentenced him to 25 years in prison.
- **NBIB Contract Background Investigator Sentenced for Impersonating a Police Officer.** The NBIB Integrity Assurance office alerted us that a contract background investigator allegedly impersonated a Federal agent while serving documents as part of a personal process server/bail bondsman business, including wearing his NBIB badge and carrying a holstered but unconcealed handgun. In August 2019, the background investigator pled no contest in the District Court of Maryland in Prince George's County to impersonating a police officer. He was sentenced to 3 years of probation.

Falsified Reports of Investigation

- **NBIB Investigator Loses Top Secret Clearance for Falsifying 90 Reports of Investigation.** An investigative review found an NBIB background investigator allegedly falsified approximately 90 reports of investigation between September 2015 and October 2016. The associated loss to OPM totaled $213,407. The background investigator's Top Secret security clearance was suspended, and he was removed from his position with NBIB. In May 2019, the background investigator pled guilty in the U.S. District Court for the District of Columbia to making a false statement. The background investigator's sentencing will be reported in a future semiannual report.
- **Contract Background Investigator Pleads Guilty to Wire Fraud, and Making False Statements Related to Falsifications.** In May 2014, we received a referral from NBIB alleging that a contract background investigator submitted false and inaccurate reports of investigation between May 2013 and May 2014. The recovery cost totaled $126,693. In January 2019, the contract background investigator was indicted in the U.S. District Court for the District of Columbia, on charges of wire fraud and making false statements. He pled guilty in April 2019. In July 2019, he was sentenced to 5 months of incarceration and 36 months of supervised release, as well as full restitution of $126,693 to OPM.

Integrity of OPM Programs

A fundamental purpose of the OIG is to investigate fraud, waste, abuse, and misconduct within OPM, its programs, and its related contracts. In addition to the criminal and civil investigations, we also conduct administrative investigations. As per the Inspector General Act of 1978, as amended, we must report to Congress by

the Semiannual Report cases involving senior positions within OPM.[11]

Administrative Investigations into Senior OPM Officials			
Senior Official	**Allegation**	**Date of Prosecutorial Declination**	**Case Summary Page**
Federal Executive Institute (FEI) Senior Official	Prohibited Personnel Practices	August 14, 2017 January 24, 2018	Page 27
OCIO Senior Official	False Statements	January 29, 2019	Page 20

In addition to the FEHBP, Retirement, and other programs previously discussed, we also investigate cases involving the CFC and other OPM programs.

The cases we investigate—including those involving OPM employees and contractors and within our other areas of oversight—are often referred to us through the OIG Hotline. Integrity investigations may involve whistleblowers and/or allegations of retaliation, and are an important part of the OIG mission to provide independent oversight and reduce program vulnerabilities.

The following case summaries highlight our investigative efforts to protect the integrity of OPM programs and the agency.

- **Case Update: Federal Executive Institute (FEI) Senior Official Referred to Office of Special Counsel for Inappropriate Hiring Practices.** In our Semiannual Report for October 1, 2018, through March 31, 2019, we reported that a senior official at OPM's (FEI) was referred to the then Acting Director and the U.S. Office of Special Counsel because of prohibited personnel practices involving the hiring and promotion of a faculty member. Specifically, we found that the friendship and status as neighbors created a reasonable conclusion that the subject senior official provided professional introductions, encouraged the hiring, and advocated for the promotion/conversion to full-time status based on that friendship. To date, we have not received a response from OPM.
- **$21,000 in CFC Funds Recovered from Alleged Charity Fraud.** The CFC reported potential fraud by a foundation allegedly entered and approved into the 2013 and 2014 CFC by the Principal Combined Fund Organization prior to being approved as a 501(c)(3) nonprofit by the Internal Revenue Service (IRS). The alleged fraud involved using a similar-sounding charity's Employer Identification Number and forging or altering official IRS documentation. The case was declined for prosecution, but our investigators recovered $21,012 held in a fund related to the supposed charity. These funds were returned to the CFC.

11 This includes the above-reported case, "Timely Notification of Data Risks and Integrity Investigation of Senior OCIO Official."

Administrative Sanctions of FEHBP Healthcare Providers

Under the FEHBP administrative sanctions authority, 5 U.S.C. § 8902a, we suspend or debar healthcare providers whose actions demonstrate that they are not sufficiently professionally responsible to participate in the FEHBP. At the end of the reporting period, there were 36,324 active suspensions and debarments from the FEHBP.

During the reporting period, our office issued 489 administrative sanctions–including both suspensions and debarments–of healthcare providers who have committed violations that impact the FEHBP and its enrollees. In addition, we responded to 2,053 sanctions-related inquiries.

Debarment disqualifies a healthcare provider from receiving payment of FEHBP funds for a stated period of time. The FEHBP has 18 bases for debarment. The most frequently cited provisions are for criminal convictions or professional licensure restrictions or revocations. Before debarring a provider, our office gives the provider prior notice and the opportunity to contest the sanction in an administrative proceeding.

Suspension has the same effect as a debarment, but it becomes effective upon issuance, without prior notice or process and is for a limited time period. The 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.

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

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

Administrative sanctions serve a protective function for the FEHBP, as well as Federal employees, annuitants, and their family members who obtain their health insurance coverage through the FEHBP.

The following cases handled during the reporting period highlight the importance of the Administrative Sanctions Program.

New York Physician and Medical Facility Debarred for Healthcare Fraud

In April 2019, our office debarred from the FEHBP a New York physician based on his conviction in the United States District Court for the Eastern District of New York healthcare fraud under 18 U.S.C. § 1347.

The charges stemmed from a scheme in which the physician submitted claims to Medicare and private insurance companies for procedures he did not perform, including skin grafts, wound packing, and foot and ankle surgery. Between 2013 and 2017, the physician caused a loss of approximately $870,000 to the Medicare program and other private and Government health insurance entities.

The physician was arraigned and pled guilty to the aforementioned charge in June 2018. The physician admitted to participating in kickback schemes that bilked Medicare and Medicaid of $163 million.

In July 2019, the physician was convicted and sentenced to one year and a day in prison for his role in a healthcare fraud scheme. The Court also ordered him to pay restitution of $869,651, a $50,000 fine, and to forfeit $177,000.

Under the FEHBP's administrative sanctions statutory authority, a conviction constitutes a mandatory basis for debarment. Our office debarred the physician for three years. In addition, the physician and his brother owned a medical facility that was used in committing the fraudulent activities. Based upon ownership and control, our office debarred the medical facility for three years. This case was referred to our office by the BCBS Association.

Ohio Physician Debarred after Suspension of Medical License

In August 2019, our office debarred from the FEHBP an Ohio anesthesiologist after his license was suspended by the Ohio Medical Board (Medical Board) after an investigation revealed he repeatedly ordered fatal dosages of painkillers for patients. The Medical Board determined that there was clear and convincing evidence the physician violated state laws and that allowing him to continue practicing medicine would present a danger and serious harm to the public.

An investigation by the Medical Board found the physician violated the following provisions of Ohio Revised Code:

- Section 4731.22(B)(2)–failure to maintain minimal standards applicable to the selection or administration of drugs, or failure to employ acceptable scientific methods in the selection of drugs or other modalities for treatment of disease; and,
- Section 4731.22(B)(6)–failure to conform to minimal standards of care of similar practitioners under the same or similar circumstances whether or not actual injury to a patient is established.

The physician was indicted on 25 counts of murder by the Franklin County, Ohio, Prosecuting Attorney's Office. The indictment alleges that from February 2015 through November 2018, he caused the death of 25 patients at two hospitals in Columbus, Ohio. The physician was arrested after a six-month criminal investigation proved he knowingly ordered potentially lethal doses of the painkiller fentanyl for patients with no other purpose than to hasten their deaths. Investigators discovered he had ordered doses that were 10–20 and even 40-times more than deemed appropriate. The physician is currently incarcerated and is still awaiting trial.

Federal regulations state that OPM may debar providers of healthcare services from participating in the FEHBP when the provider's license to provide a healthcare 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 will remain in effect for an indefinite period pending the resolution of his medical license and outcome of his trial. This case was referred to our office by the BCBS Association.

Louisiana Physician, Medical Billing Supervisor, and Pain Management Clinic Debarred for Healthcare Fraud

FEHBP regulations define a healthcare provider as any person/entity that furnishes healthcare services or supplies, either directly or indirectly. "Hands-on" providers such as physicians, dentists, psychologists, pharmacists/pharmacies, hospitals, and clinics fall within this definition. In cases involving false claims, our office also considers office managers and billing services to be "indirect" providers when they knowingly facilitate, create, submit, or assist in any of the wrongful activities associated with the violations. In addition, based on the

provider's ownership or control interest, we may sanction their entity.

In July 2019, our office debarred from the FEHBP a Louisiana physician and his medical billing supervisor because both were convicted of healthcare fraud in the United States District Court for the Middle District of Louisiana. This case was referred to our office from the BCBS Association.

The physician co-owned and served as medical director of a pain management clinic in Baton Rouge, Louisiana. The indictment alleged that from about June 2005 through March 2015, the physician and the medical billing supervisor created a scheme to obtain higher reimbursement payments from Medicare and other healthcare insurers through submission of fraudulent claims. The physician falsified medical records to support the fraudulent claims and directed other staff to do the same. The fraudulent claims indicated office visits and the related minor surgical procedures occurred on different days when, in fact, the surgeries and office visits occurred on the same day. This was done so the physician could claim higher reimbursement payments for separate office visits that did not occur. This practice, commonly referred to as "unbundling," was done to defraud healthcare insurers.

In February 2019, the physician pled guilty to one count of conspiracy to commit healthcare fraud. The medical billing supervisor pled guilty to one count of conspiracy to commit healthcare fraud and wire fraud, and two counts of healthcare fraud. They are still awaiting sentencing.

The conviction forms a mandatory basis for debarment under the FEHBP's administrative sanctions authority. Therefore, our office debarred the physician and the medical billing supervisor for a period of three years. Also, our office debarred the physician's pain management clinic, which was used in committing the fraudulent activities, for three years.

Evaluation Activities

The Office of Evaluations provides an alternative method for conducting independent, credible, and thorough reviews of OPM's programs and operations to prevent fraud, waste, and abuse. The Office of Evaluations quickly analyzes OPM concerns or issues that need immediate attention by using a variety of review methods and evaluation techniques. The work done by the Office of Evaluations is completed in accordance with the Quality Standards for Inspection and Evaluation (known as the Blue Book) published by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). Our evaluation reports provide OPM management with findings and recommendations that will assist in enhancing program operations, efficiency, effectiveness, and compliance with applicable policies and procedures.

We completed one program evaluation during this reporting period, which is discussed below.

OPM's Employee Services' Senior Executive Service and Performance Management Office

Washington, D.C.
Report Number 4K-ES-00-18-041
July 1, 2019

Our analysts completed an evaluation of OPM's Employee Services' Senior Executive Service and Performance Management office (SESPM). This office manages the overall Federal personnel program relating to Senior Executive Service (SES) and senior professionals (Senior Level and Scientific or Professional). The Civil Service Reform Act of 1978 established the SES as a separate personnel system that applies the same executive qualification requirements to all of its members.

Over the years, stakeholders offered various ideas and suggestions to improve SES operations. Since its creation, a few statutory changes were implemented; however, stakeholders continued to call for further improvements to the efficiency and management of operations and processes. As a result, we conducted this evaluation to determine whether OPM's Employee Services has controls in place to effectively carry out its mission, providing oversight and assistance to Federal agencies for their SES and performance management needs.

We determined that SESPM needs to strengthen its controls over the administration of the Qualifications Review Board (QRB) process and enhance its oversight of the certification process for SES performance appraisal systems. Specifically, SESPM management needs to:

- Build ongoing monitoring and quality control measures to ensure its staff complies with laws and regulations, reports complete and accurate data, and maintains adequate support documentation;
- Update and finalize its standard operating procedures, QRB Charter, and reference guide to ensure supervisory review processes are included and activities aligned with their common practices, including maintaining support documentation; and
- Assemble working groups with appropriate stakeholders to collaborate, brainstorm, and develop ways to improve the QRB process and the SES performance appraisal systems.

We made six recommendations to improve controls and enhance oversight. Since the conclusion of our fieldwork,

the SESPM planned actions to address these issues and recommendations. However, we consider the recommendations open until corrective actions have been implemented.

Legislative Activities

Under the Inspector General Act of 1978, as amended, each statutory Inspector General must obtain legal advice from a counsel either reporting directly to the Inspector General or another Inspector General. Thus, the OIG's Office of Legal and Legislative Affairs advises the Inspector General and other OIG components on legal and regulatory matters, as well as develops and reviews legislative proposals to prevent and reduce fraud, waste, and abuse in OPM programs and operations. We also submit comments on proposed and draft legislation to the Inspector General, Congress, and the CIGIE Legislative Committee.

During this reporting period, the OIG provided technical comments to the Senate Committee on Homeland Security and Governmental Affairs on the Representative Payee Fraud Prevention Act of 2019, S. 1430, 116th Congress (2019). The legislation was introduced in May 2019 and reported out of Committee in July 2019. The Deputy Inspector General Performing the Duties of the Inspector General also testified before the House Committee on Oversight and Reform Subcommittee on Government Operations.

Cracking Down on Federal Retirement Benefit Fraud

The OPM OIG is encountering a rising number of cases involving Federal retirement benefit fraud and misuse by representative payees.[12] However, the statutory authority necessary for Federal prosecution is deficient. Currently, embezzlement or conversion of Social Security and veterans benefits by representative payees is a Federal felony, but the same embezzlement or conversion of benefits provided to Federal retirees through the Federal retirement system is not.[13]

The Representative Payee Fraud Prevention Act of 2019 provides a legislative solution to close this loophole.[14] This bipartisan bill will give the OPM OIG a clear statutory authority to propose Federal felony prosecution of representative payees who misuse funds from OPM-administered retirement programs.[15] Classifying this crime as a felony is necessary to protect retirees and their hard-earned retirement benefits from dishonest caretakers who fail to use the allotted payments for the retiree's benefit.

As of September 30, 2019, there were approximately 15,800 individuals registered with OPM as representative payees between two OPM-administered retirement programs, CSRS and FERS. With the passage of the Representative Payee Fraud Prevention Act of 2019, Federal prosecutors will be able to prosecute individuals abusing the Federal retirement system and deter unscrupulous behavior, affording OPM payees the same safeguards as Social Security and veteran payees.

12 A representative payee is an individual authorized to receive payments on behalf of a Federal annuitant who is unable to manage his or her own finances. 5 U.S.C. §§ 8345(e), 8466(c).

13 42 U.S.C. §§ 408, 1383a; 38 U.S.C. § 6101.

14 Representative Payee Fraud Prevention Act of 2019, S.1430, 116th Congress (2019-2020).

15 The primary retirement funds administered by OPM are the FERS and the CSRS.

Testifying Before House Committee on Oversight and Reform

On May 22, 2019, the House Committee on Oversight and Reform Subcommittee on Government Operations held a hearing entitled "The Administration's War on a Merit Based Civil Service." The hearing examined the Administration's proposal to eliminate funding from OPM and move its offices and operations into the Department of Defense, the General Services Administration, and the Executive Office of the President.

In his testimony, the Deputy Inspector General Performing the Duties of the Inspector General addressed the transfer of the background investigation function to the Department of Defense and the Administration's proposed transfer of OPM to GSA. While he did not raise concerns regarding the NBIB transfer, he discussed the OIG's concern with the proposed transfer of OPM to GSA. Specifically, the OIG was and remains concerned that OPM appeared to be making decisions related to the proposed transfer without conducting adequate evidence-based analysis. Moreover, the documentation OPM provided to the OIG fails to deliver the data and analysis necessary for the OIG to assess whether this proposal will promote or improve economy, efficiency, and effectiveness in the administration of OPM programs.

OPM and GSA must at a minimum conduct a workforce planning analysis and a comprehensive financial analysis of the potential costs of and savings from such a substantial reorganization. As noted by the U.S. Government Accountability Office in a recent report on Government reorganizations, "the use of data and evidence is critical from setting program priorities and allocating resources to taking corrective action to solve performance problems and ultimately improve results."[16] The absence of careful analysis and objective planning based on solid financial and workforce data increases the likelihood of wasting taxpayer dollars; disrupting the administration of benefit programs relied upon by Federal employees, annuitants, and their families; and potentially undermining the civil service.

16 GAO, *Government Reorganization: Key Questions to Assess Agency Reform Efforts*, GAO-18-427 (Washington, D.C., June 13, 2018), at page 11 (internal citations omitted).

Statistical Summary of Enforcement Activities

INVESTIGATIVE ACTIONS AND RECOVERIES:

Indictments and Informations	56
Arrests	42
Convictions	56
Criminal Complaints/Pre-Trial Diversion	4
Subjects Presented for Prosecution	193
Federal Venue	189
Criminal	42
Civil	147
State Venue	0
Local Venue	4

Expected Recovery Amount to OPM Programs	$20,244,044
Civil Judgments and Settlements	$13,799,023
Criminal Fines, Penalties, Assessments, and Forfeitures	$1,468,359
Administrative Recoveries	$4,956,662
Expected Recovery Amount for All Programs and Victims[17]	$1,216,233,579

INVESTIGATIVE ADMINISTRATIVE ACTIONS:

FY 2019 Investigative Reports Issued[18]	313
Whistleblower Retaliation Allegations Substantiated	0
Cases Referred for Suspension and Debarment	2
Healthcare Cases Referred to the OIG for Suspension and Debarment	2
NBIB Cases Referred to OPM for Suspension and Debarment	0
Personnel Suspensions and Terminations	1
Referral to the OIG's Office of Audits	0
Referral to OPM Program Office	43

17 This figure represents criminal fines/penalties and civil judgments/settlements returned not to OPM, but to the general fund of the Treasury. It also includes asset forfeitures, 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 credit for the fines, penalties, assessments, and forfeitures.

18 The total number of investigative reports issued during the reporting period includes reports of investigations and summative investigative reports.

Administrative Sanctions Activities:

FEHBP Debarments and Suspensions Issued 489

FEHBP Provider Debarment and Suspension Inquiries 2,053

FEHBP Debarments and Suspensions in Effect at End of Reporting Period 36,324

OIG Investigative Case Activity

	Healthcare and Insurance	Retirement Services	Other OPM Program Offices	External/ Internal Matters	Total
Cases Opened	367	75	15	6	463
Investigations	43	13	3	1	60
Complaints	324	62	12	5	403
Inquiries Opened	1023	2	0	0	1025
Referrals – FEHBP Carriers/Program Office	773	0	0	0	773
Referrals – All Other Sources/Proactive	250	2	0	0	252
Cases Closed	224	86	5	10	325
Investigations	35	14	1	3	53
Complaints	189	72	4	7	272
Inquiries Closed[19]	989	3	0	1	993
Referrals – FEHBP Carriers/Program Office	763	0	0	0	763
Referrals – All Other Sources/Proactive	226	3	0	1	230
Cases In-Progress[20]	793	103	37	17	950
Investigations	207	46	13	8	274
Complaints	586	57	24	9	676
Inquiries In-Progress[21]	414	2	0	0	416
Referrals – FEHBP Carriers/Program Office	389	1	0	0	390
Referrals – All Other Sources/Proactive	25	1	0	0	26

19 Cases closed may have been opened in a previous reporting period.

20 Cases in progress may have been opened in a previous reporting period.

21 Inquiries in progress may have been opened in a previous reporting period.

OIG Hotline Case Activity

OIG Hotline Cases Received . . . 1339

Sources of OIG Hotline Cases Received

- Website . . . 735
- Telephone . . . 397
- Letter . . . 124
- Email . . . 83
- In-Person . . . 0

By OPM Program Office

- Healthcare and Insurance . . . 227
  - Customer Service . . . 138
  - Billing Disputes . . . 5
  - Other Healthcare and Insurance Issues . . . 84
- Retirement Services . . . 260
  - Customer Service . . . 223
  - Annuity Calculation . . . 1
  - Other Retirement Services Issues . . . 36
- Other OPM Program Offices/Internal Matters . . . 79
  - Customer Service . . . 45
  - Other OPM Program/Internal Issues . . . 21
  - Employee or Contractor Misconduct . . . 13
- External Agency Issues (not OPM-related) . . . 773

OIG Hotline Cases Reviewed and Closed . . . 1085

Outcome of OIG Hotline Cases Closed

- Referred to External Agency . . . 545
- Referred to OPM Program Office . . . 253
  - Retirement Services . . . 139
  - Healthcare and Insurance . . . 71
  - Other OPM Programs/Internal Matters . . . 43
- No Further Action . . . 278
- Converted to a Case . . . 9

OIG Hotline Cases Pending[22] 254

By OPM Program Office

22 Includes hotline cases pending an OIG internal review or an agency response to a referral.

APPENDIX I – A
Final Reports Issued with Questioned Costs for Insurance Programs
April 1, 2019 to September 30, 2019

	Subject	Number of Reports	Questioned Costs
A.	Reports for which no management decision had been made by the beginning of the reporting period	5	$63,341,047
B.	Reports issued during the reporting period with findings	4	$27,805,879
	Subtotals (A+B)	9	$91,146,926
C.	Reports for which a management decision was made during the reporting period:	5	$7,119,658
	1. Disallowed costs	N/A	$6,105,734
	2. Costs not disallowed	N/A	$1,013,924[1]
D.	Reports for which no management decision has been made by the end of the reporting period	4	$84,027,268
E.	Reports for which no management decision has been made within 6 months of issuance	2	$62,044,464

[1]Represents the net costs, which includes overpayments and underpayments, to insurance carriers. Underpayments are held (not returned to insurance carriers) until overpayments are recovered.

APPENDIX I – B
Final Reports Issued with Questioned Costs for All Other Audit Entities
April 1, 2019 to September 30, 2019

	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	0	$0
	Subtotals (A+B)	0	$0
C.	Reports for which a management decision was made during the reporting period:	0	$0
	1. Disallowed costs	N/A	$0
	2. Costs not disallowed	N/A	$0
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 II

Resolution of Questioned Costs in Final Reports for Insurance Programs
April 1, 2019 to September 30, 2019

	Subject	Questioned Costs
A.	Value of open recommendations at the beginning of the reporting period	$107,551,898
B.	Value of new audit recommendations issued during the reporting period	$27,805,879
	Subtotals (A+B)	$135,357,777
C.	Amounts recovered during the reporting period	$6,765,361
D.	Amounts allowed during the reporting period	$6,204,571
E.	Other adjustments	$0
	Subtotals (C+D+E)	$12,969,932
F.	Value of open recommendations at the end of the reporting period	$122,387,845

APPENDIX III

Final Reports Issued with Recommendations for Better Use of Funds
April 1, 2019 to September 30, 2019

	Subject	Number of Reports	Dollar Value
A.	Reports for which no management decision had been made by the beginning of the reporting period	1	$108,880,417
B.	Reports issued during the reporting period with findings	0	0
	Subtotals (A+B)	1	$108,880,417
C.	Reports for which a management decision was made during the reporting period	0	0
D.	Reports for which no management decision has been made by the end of the reporting period	1	$108,880,417
E.	Reports for which no management decision has been made within 6 months of issuance	1	$108,880,417

APPENDIX IV
Insurance Audit Reports Issued
April 1, 2019 to September 30, 2019

Report Number	Subject	Date Issued	Questioned Costs
1C-JK-00-18-029	TakeCare Insurance Company, Inc., in Tamuning, Guam	April 25, 2019	$20,627,290
1C-LX-00-18-031	Blue Care Network of Michigan in Southfield, Michigan	June 4, 2019	$0
1N-0A-00-18-048	Flexible Spending Account for Federal Employees as Administered by Automatic Data Processing, Inc., for Contract Years 2011 through 2016 in Louisville, Kentucky	June 18, 2019	$0
1A-10-09-18-050	BlueCross BlueShield of Alabama in Birmingham, Alabama	July 11, 2019	$4,684,247
1G-LT-00-19-003	Federal Long Term Care Insurance Program Operations as Administered by Long Term Care Partners, LLC, for Contract Years 2013 through 2016 in Portsmouth, New Hampshire	July 17, 2019	$0
1A-99-00-18-045	Pension, Post-Retirement Benefit, and Affordable Care Act Costs for a Sample of BlueCross and/or BlueShield Companies in Washington, D.C.	August 7, 2019	$1,138,828
1J-0D-00-19-030	Aetna Dental's 2020 Premium Rate Proposal for the Federal Employees Dental and Vision Insurance Program in Blue Bell, Pennsylvania	August 9, 2019	$0
1G-LT-00-18-040	BENEFEDS as Administered by Long Term Care Partners, LLC, for Contract Years 2014 through 2016 in Portsmouth, New Hampshire	September 11, 2019	$0
1A-99-00-19-001	Coordination of Benefits with Medicare for BlueCross and BlueShield Plans Fiscal Year 2018 in Washington, D.C.	September 19, 2019	$1,355,514
TOTAL			$27,805,879

APPENDIX V
Internal Audit Reports Issued
April 1, 2019 to September 30, 2019

Report Number	Subject	Date Issued
4A-CF-00-19-012	The U.S. Office of Personnel Management's Fiscal Year 2018 Improper Payments Reporting in Washington, D.C.	June 3, 2019
4A-HR-00-19-034	Independent Certified Public Accountants on the U.S. Office of Personnel Management Human Resources Solutions' Schedule of Assets and Liabilities in Washington, D.C.	June 6, 2019
4A-IS-00-19-035	Independent Certified Public Accountants on the U.S. Office of Personnel Management National Background Investigations Bureau's Details of Analysis and Assumptions Schedule in Washington, D.C.	June 6, 2019

APPENDIX VI
Information Systems Audit Reports Issued
April 1, 2019 to September 30, 2019

Report Number	Subject	Date Issued
4A-CI-00-18-037	The U.S. Office of Personnel Management's Compliance with the Federal Information Technology Acquisition Reform Act in Washington, D.C.	April 25, 2019
lA-10-32-18-046	Information Systems General and Application Controls at Blue Cross Blue Shield of Michigan in Detroit, Michigan	May 16, 2019
4A-CI-00-19-006	Information Technology Security Controls of the U.S. Office of Personnel Management's Enterprise Human Resource Integration Data Warehouse in Washington, D.C.	June 17, 2019
1C-59-00-19-005	Information Systems General and Application Controls at Kaiser Foundation Health Plan, Inc., Northern and Southern California Regions in Downey and Corona, California	July 23, 2019

APPENDIX VII
Evaluation Reports Issued
April 1, 2019 to September 30, 2019

Report Number	Subject	Date Issued
4K-ES-00-18-041	Evaluation of the U.S. Office of Personnel Management's Employee Services' Senior Executive Service and Performance Management Office in Washington, D.C.	July 1, 2019

APPENDIX VIII

Summary of Reports More than Six Months Old Pending Corrective Action as of September 30, 2019

Report Number	Subject	Date Issued	Recommendations	
			Open	Total
4A-CI-00-08-022	Federal Information Security Management Act for Fiscal Year 2008 in Washington, D.C.	September 23, 2008	2	19
4A-CF-00-08-025	The U.S. Office of Personnel Management's Fiscal Year 2008 Consolidated Financial Statements in Washington, D.C.	November 14, 2008	1	6
4A-CI-00-09-031	Federal Information Security Management Act for Fiscal Year 2009 in Washington, D.C.	November 5, 2009	2	30
4A-CF-00-09-037	The U.S. Office of Personnel Management's Fiscal Year 2009 Consolidated Financial Statements in Washington, D.C.	November 13, 2009	1	5
4A-CF-00-10-015	The U.S. Office of Personnel Management's Fiscal Year 2010 Consolidated Financial Statements in Washington, D.C.	November 10, 2010	3	7
4A-CI-00-10-019	Federal Information Security Management Act for Fiscal Year 2010 in Washington, D.C.	November 10, 2010	2	41
1K-RS-00-11-068	Stopping Improper Payments to Deceased Annuitants in Washington, D.C.	September 14, 2011	2	14
4A-CI-00-11-009	Federal Information Security Management Act for Fiscal Year 2011 in Washington, D.C.	November 9, 2011	2	29
4A-CF-00-11-050	The U.S. Office of Personnel Management's Fiscal Year 2011 Consolidated Financial Statements in Washington, D.C.	November 14, 2011	1	7
4A-CI-00-12-016	Federal Information Security Management Act for Fiscal Year 2012 in Washington, D.C.	November 5, 2012	3	18
4A-CF-00-12-039	The U.S. Office of Personnel Management's Fiscal Year 2012 Consolidated Financial Statements in Washington, D.C.	November 15, 2012	1	3
4A-CI-00-13-021	Federal Information Security Management Act for Fiscal Year 2013 in Washington, D.C.	November 21, 2013	4	16
4A-CF-00-13-034	The U.S. Office of Personnel Management's Fiscal Year 2013 Consolidated Financial Statements in Washington, D.C.	December 13, 2013	1	1
4A-CI-00-14-015	Information Technology Security Controls of the U.S. Office of Personnel Management's Development Test Production General Support System Fiscal Year 2014 in Washington, D.C.	June 6, 2014	2	6
4A-CF-00-14-039	The U.S. Office of Personnel Management's Fiscal Year 2014 Consolidated Financial Statements in Washington, D.C.	November 10, 2014	3	4
4A-CI-00-14-016	Federal Information Security Management Act for Fiscal Year 2014 in Washington, D.C.	November 12, 2014	14	29
4K-RS-00-14-076	The Review of the U.S. Office of Personnel Management's Compliance with the Freedom of Information Act in Washington, DC	March 23, 2015	2	3
4A-RS-00-13-033	Assessing the Internal Controls over the U.S. Office of Personnel Management's Retirement Services' Retirement Eligibility and Services Office in Washington, D.C.	April 13, 2015	1	7

APPENDIX VIII

Summary of Reports More than Six Months Old Pending Corrective Action as of September 30, 2019

Report Number	Subject	Date Issued	Recommendations	
			Open	Total
4A-CI-00-15-055	Flash Audit Alert – The U.S. Office of Personnel Management's Infrastructure Improvement in Washington, D.C.	June 17, 2015	1	2
4A-RI-00-15-019	Information Technology Security Controls of the U.S. Office of Personnel Management's Annuitant Health Benefits Open Season System in Washington, D.C.	July 29, 2015	2	7
4A-CI-00-15-011	Federal Information Security Modernization Act for Fiscal Year 2015 in Washington, D.C.	November 10, 2015	15	27
4A-CF-00-15-027	The U.S. Office of Personnel Management's Fiscal Year 2015 Consolidated Financial Statements in Washington, D.C.	November 13, 2015	5	5
1A-10-17-14-037	Healthcare Service Corporation in Chicago, Illinois	November 19, 2015	3	16
4A-CF-00-16-026	The U.S. Office of Personnel Management's Fiscal Year 2015 Improper Payments Reporting in Washington, D.C.	May 11, 2016	1	6
4A-CI-00-16-037	Second Interim Status Report on the U.S. Office of Personnel Management's Infrastructure Improvement Project - Major IT Business Case in Washington, D.C.	May 18, 2016	2	2
4A-CA-00-15-041	The U.S. Office of Personnel Management's Office of Procurement Operations' Contract Management Process in Washington, D.C.	July 8, 2016	5	6
1C-L4-00-I6-013	HMO Health Ohio in Cleveland, Ohio	September 23, 2016	2	2
4K-RS-00-16-023	The U.S. Office of Personnel Management's Retirement Services' Customer Service Function in Washington, D.C.	September 28, 2016	2	3
4A-CI-00-16-061	Web Application Security Review in Washington, D.C.	October 13, 2016	4	4
4A-CI-00-16-039	Federal Information Security Modernization Act for Fiscal Year 2016 in Washington, D.C.	November 9, 2016	20	26
lA-10-33-15-009	Blue Cross and Blue Shield of North Carolina in Durham, North Carolina	November 10, 2016	3	6
4A-CF-00-16-030	The U.S. Office of Personnel Management's Fiscal Year 2016 Consolidated Financial Statements in Washington, D.C.	November 14, 2016	15	19
4A-RS-00-16-035	Information Security Controls of the U.S. Office of Personnel Management's Federal Annuity Claims Expert System in Washington, D.C.	November 21, 2016	2	13
4A-CF-00-17-012	The U.S. Office of Personnel Management's Fiscal Year 2016 Improper Payments Reporting in Washington, D.C.	May 11, 2017	1	10
4A-CI-00-17-014	The U.S. Office of Personnel Management's Security Assessment and Authorization Methodology in Washington, D.C.	June 20, 2017	4	4
4A-OO-00-16-046	The U.S. Office of Personnel Management's Purchase Card Program in Washington, D.C.	July 7, 2017	2	12
4A-CF-00-17-044	Information Technology Security Controls of the U.S. Office of Personnel Management's Federal Financial System in Washington, D.C.	September 29, 2017	2	9

APPENDIX VIII

Summary of Reports More than Six Months Old Pending Corrective Action as of September 30, 2019

Report Number	Subject	Date Issued	Recommendations	
			Open	Total
4A-CI-00-17-030	Information Technology Security Controls of the U.S. Office of Personnel Management's SharePoint Implementation in Washington, D.C.	September 29, 2017	8	8
4A-CI-00-17-020	Federal Information Security Modernization Act Audit Fiscal Year 2017 in Washington, D.C.	October 27, 2017	36	39
4A-CF-00-17-028	The U.S. Office of Personnel Management's Fiscal Year 2017 Consolidated Financial Statements in Washington, D.C.	November 13, 2017	18	18
4A-CF-00-15-049	The U.S. Office of Personnel Management's Travel Card Program in Washington, D.C.	January 16, 2018	19	21
4A-CI-00-18-022	Management Advisory Report - The U.S. Office of Personnel Management's Fiscal Year 2017 IT Modernization Expenditure Plan in Washington, D.C.	February 15, 2018	4	4
1A-99-00-16-021	Global Veterans Affairs Claims for Blue Cross and Blue Shield Plans in Washington, D.C.	February 28, 2018	5	5
4K-RS-00-17-039	The U.S. Office of Personnel Management's Retirement Services' Imaging Operations in Washington, D.C.	March 14, 2018	1	3
4A-CF-00-16-055	The U.S. Office of Personnel Management's Common Services in Washington, D.C.	March 29, 2018	5	5
4A-CF-00-18-012	The U.S. Office of Personnel Management's Fiscal Year 2017 Improper Payments Reporting in Washington, D.C.	May 10, 2018	1	2
4A-HR-00-18-013	Information Technology Security Controls of the U.S. Office of Personnel Management's USA Staffing System in Washington, D.C.	May 10, 2018	2	4
4A-CI-00-18-044	U.S. Office of Personnel Management's Fiscal Year 2018 IT Modernization Expenditure Plan in Washington, D.C.	June 20, 2018	2	2
4A-PP-00-18-011	Information Technology Security Controls of the U.S. Office of Personnel Management's Health Claims Data Warehouse in Washington, D.C.	June 25, 2018	2	12
4A-CI-00-18-038	Federal Information Security Modernization Act Audit Fiscal Year 2018 in Washington, D.C.	October 30, 2018	44	52
4A-CF-00-18-024	The U.S. Office of Personnel Management's Fiscal Year 2018 Consolidated Financial Statements in Washington, D.C.	November 15, 2018	23	23
4K-CI-00-18-009	The U.S. Office of Personnel Management's Preservation of Electronic Records in Washington, D.C.	December 21, 2018	1	3
1C-UX-00-18-019	Information Systems General and Application Controls at Medical Mutual of Ohio in Cleveland, Ohio	January 24, 2019	3	12
1C-P2-00-18-014	Presbyterian Health Plan in Albuquerque, New Mexico	March 7, 2019	3	16

APPENDIX IX

Most Recent Peer Review Results as of September 30, 2019

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

Subject	Date of Report	Result
System Review Report on the Audit Organization of the Office of Inspector General for the U.S. Office of Personnel Management (Issued by the U.S. Department of Commerce Office of Inspector General)	October 4, 2018	Pass[1]
System Review Report on the NASA Office of Inspector General Audit Organization (Issued by the Office of the Inspector General, U.S. Office of Personnel Management)	August 13, 2018	Pass
Quality Assessment Review of the Investigative Operations of the Office of the Inspector General for the National Science Foundation (Issued by the Office of the Inspector General, U.S. Office of Personnel Management)	December 14, 2017	Compliant[2]
Quality Assessment Review of the Investigative Operations of the Office of the Inspector General for the U.S. Office of Personnel Management (Issued by the Office of Inspector General, Corporation for National and Community Service)	December 2, 2016	Compliant

[1]A 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.

[2]A 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.

APPENDIX X
Investigative Recoveries
April 1, 2019 to September 30, 2019

Statistic Type	Program Office	Type of Recovery	Total Recovery Amount	Total OPM Net
Administrative			$15,187,056	$4,956,662
	Healthcare and Insurance		$13,989,140	$3,758,746
		Collection of Improper Payments	$13,989,140	$3,758,746
	National Background Investigations Bureau		$136,776	$136,776
		Contract Off-Sets	$136,776	$136,776
	Merit Systems (Combined Federal Campaign) **Administrative** **Recovery** **Retirement Services**		$21,012 $21,012 $1,040,128	$21,012 $21,012 $1,040,128
		Admin Debt Recoveries	$918,296	$918,296
		Bank Reclamations	$118,497	$118,497
		Identification of Improper Payments	$3,335	$3,335
Civil			$1,196,417,347	$13,799,023
	Healthcare and Insurance		$1,196,417,347	$13,799,023
		Civil Actions	$1,196,417,347	$13,799,023
Criminal			$4,629,176	$1,468,359
	Healthcare and Insurance		$3,043,365	$539,993
		Court Assessments/Fees	$0	$0
		Criminal Fines	$300	$0
		Criminal Judgments/Restitution	$3,043,065	$539,993
	National Background Investigations Bureau		$212,964	$212,407
		Court Assessments/Fees	$557	$0
		Criminal Judgments/Restitution	$212,407	$212,407
	Retirement Services		$1,372,847	715,959
		Court Assessments/Fees	$1,300	$0
		Criminal Judgments/Restitution	$1,371,547	$0
Grand Total			$1,216,233,579	$20,224,044

INDEX OF REPORTING REQUIREMENTS
(Inspector General Act of 1978, As Amended)

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

For additional information or copies of this publication, please contact:

OFFICE OF THE INSPECTOR GENERAL

U.S. OFFICE OF PERSONNEL MANAGEMENT

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

Telephone: (202) 606–1200
Fax: (202) 606–2153
www.opm.gov/our-inspector-general/

September 2019
OIG–SAR–61