U.S. Office of Personnel Management

Office of the Inspector General

Semiannual Report to Congress

October 1, 2019 March 31, 2020

PRODUCTIVITY INDICATORS

FINANCIAL IMPACT

Audit Recommendations for Recovery of Funds
$11,149,664

Management Commitments to Recover Funds
$2,214,357

Recoveries Through Investigative Actions
$3,799,195

Note: OPM Management Commitments for Recovery of Funds during this reporting period reflect amounts covering current and past reporting period audit recommendations.

ACCOMPLISHMENTS

25 Audit Reports Issued

Evaluation Reports Issued **1**

Management Advisories Issued **1**

622 Investigations and Complaints Closed

Indictments and Criminal Informations **23**

27 Arrests

26 Convictions

1,092 Hotline Contacts and Complaints Received

Hotline Contacts and Complaints Closed **419**

334 Debarments and Suspensions of Providers from the Federal Employees Health Benefits Program

2,152 Debarment and Suspension Inquiries Regarding Federal Employees Health Benefits Program's Providers

MESSAGE FROM THE DEPUTY INSPECTOR GENERAL PERFORMING THE DUTIES OF THE INSPECTOR GENERAL

When I first began thinking of the Inspector General's Message for this semiannual reporting period, I was eager to highlight the Representative Payee Fraud Prevention Act of 2019, enacted by Congress and signed into law by the President on March 18, 2020. For nearly five years, the Office of the Inspector General (OIG) has worked closely with the U.S. Office of Personnel Management (OPM) and Congress on this high priority legislative proposal.

However, it is difficult to start any message without acknowledging that the 2019 novel coronavirus (COVID-19) has temporarily changed not only the way we live our lives, but also the way in which OPM and the OPM OIG perform our mission critical functions. While the OPM OIG has seamlessly transitioned to 100 percent telework, nationwide travel restrictions are making some elements of our work more difficult. Nonetheless, as we work remotely, we remain committed to combatting health care fraud and protecting Federal employees, annuitants, and their families from harm, so that they can continue to receive their earned annuity and health care benefits.

The Representative Payee Fraud Prevention Act of 2019 will certainly help the OIG accomplish our goal of holding individuals accountable if they take advantage of vulnerable Federal annuitants. We reached out to Congress in 2015 when we first identified a statutory loophole that prevented our office from pursuing dishonest Representative Payees who misused annuity payments intended for annuitants or their survivors. Through the Representative Payee program, Federal annuitants, minors, and others with qualifying disabilities who receive annuity payments from the Civil Service Retirement System (CSRS) and the Federal Employees Retirement System (FERS), may use a financial representative to assist them in managing their OPM annuity payments. OPM has the authority to make annuity payments to a "Representative Payee," a financial representative who is willing to act on behalf of the annuitant. The Representative Payee will then receive the annuity payment and is responsible for using the payment in the best interest of the annuitant.

The Representative Payee program is not unique to OPM. In fact, the U.S. Railroad Retirement Board, Social Security Administration, and the U.S. Department of Veterans Affairs all have similar programs. Yet, as we noted in our last semiannual report, embezzlement or conversion of Social Security, veterans, and other Federal annuitants' benefits by Representative Payees is a Federal felony, whereas the same embezzlement or conversion of benefits provided to Federal annuitants through the OPM-administered Federal retirement systems was not. This disparity in treatment produced devastating effects.

A number of Representative Payees misappropriate funds intended for annuitants, often depriving annuitants of food, housing, or medical care. Our office received reports that annuitants have been evicted or amassed thousands of dollars in unpaid nursing home bills because their Representative Payee inappropriately used

the annuitant's funds. In one particularly egregious case, authorities found an annuitant unconscious on the street. Once the annuitant was revived, authorities discovered that her mental capacity was diminished to the point where she was non-verbal. When the owner of the personal care home who served as the annuitant's Representative Payee was finally located, the owner refused to continue caring for the annuitant. Nonetheless, the owner continued to cash the annuitant's checks.

Prior to the passage of the Representative Payee Fraud Prevention Act of 2019, the OPM OIG was forced to abandon its pursuit of prosecution in a number of cases because of the lack of a clear statutory basis upon which to propose a Federal prosecution of the Representative Payee. However, the passage of this important legislation allows the OPM OIG to work with the Department of Justice to more fully pursue the investigation and prosecution of these cases. We are now better equipped to fulfill the Administration's priority of minimizing improper payments and protecting the Civil Service Retirement and Disability Fund.

In the context of the current public health emergency, I am grateful that a barrier to protecting Federal annuitants has been removed. In addition, I extend my gratitude to the dedicated members of the OPM OIG, who continue to adapt to how we respond to the challenges presented by COVID-19. We stand ready to continue to serve the American people, and we will continue to work with OPM and our Congressional partners in protecting the integrity of OPM services and programs through independent and objective oversight.

Norbert E. Vint

Deputy Inspector General Performing the

Duties of the Inspector General

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

PRODUCTIVITY INDICATORS ..... Inside Front Cover

MESSAGE FROM THE DEPUTY INSPECTOR GENERAL i

MISSION STATEMENT iii

FIELD OFFICES vii

AUDIT ACTIVITIES 1

- Health Insurance Carrier Audits 1
- Information Systems Audits 8
- Internal Audits 12
- Special Audits 17

ENFORCEMENT ACTIVITIES 19

- Investigative Activities 19
- Administrative Sanctions of FEHBP Health Care Providers 30

EVALUATIONS ACTIVITIES 35

LEGAL AND LEGISLATIVE ACTIVITIES 37

STATISTICAL SUMMARY OF ENFORCEMENT ACTIVITIES 39

OIG HOTLINE CASE ACTIVITY 41

APPENDICES 43

- I: Final Reports Issued with Questioned Costs for Insurance Programs 43
- II: Resolution of Questioned Costs in Final Reports for Insurance Programs 44
- III: Final Reports Issued with Recommendations for Better Use of Funds 44
- IV: Insurance Audit Reports Issued 45
- V: Internal Audit Reports Issued 46
- VI: Information Systems Audit Reports Issued 46
- VII: Special Review Reports Issued 47
- VIII: Evaluation Reports Issued 47
- IX: Summary of Reports More Than Six Months Old Pending Corrective Action 48
- X: Most Recent Peer Review Results 53
- XI: Investigative Recoveries 54

INDEX OF REPORTING REQUIREMENTS 55

OIG OFFICE LOCATIONS

AUDIT ACTIVITIES

Health Insurance Carrier Audits

The U.S. Office of Personnel Management (OPM) contracts with Federal Employees Health Benefits Program (FEHBP) carriers for health benefit plans for Federal employees, annuitants, 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 (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 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 they are paid an amount commensurate with the number of subscribing FEHBP enrollees and the premiums paid by those enrollees. 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 BlueCross BlueShield (BCBS) Service Benefit Plan), but they also offer experience-rated HMOs. These carriers are reimbursed for actual claims paid and administrative expenses incurred, and they are paid a service charge 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. Department of Treasury (Treasury) that holds premiums paid by enrollees and from which carriers are reimbursed for claims paid and expenses incurred.

Community-Rated Carriers

The community-rated carrier audit universe covers 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.

SSSG 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.

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 Medical Loss Ratio (MLR) requirement to replace the SSSG comparison requirement for most community-rated FEHBP carriers.

MLR is the portion 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. In 2012, community-rated FEHBP carriers could elect to follow the FEHBP-specific MLR requirements instead of the SSSG requirements. Beginning in 2013, the MLR methodology was required for all community-rated carriers, except those State mandated to use traditional community rating. State mandated traditional community rating carriers continue to be subject to the SSSG comparison rating methodology, which was amended in 2015 to require only one SSSG 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 health care 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.

During the current reporting period, we issued five final audit reports on community-rated health

plans participating in the FEHBP. The following summaries highlight notable audit findings from these audits

The AultCare Health Plan

Canton, Ohio
Report Number 1C-3A-00-18-052
November 25, 2019

AultCare Health Plan has participated in the FEHBP since 1996, and provides health benefits to FEHBP members in the Canton, Ohio area. The audit covered contract years 2014 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 for contract years 2014 through 2016. This resulted in overstated MLR credits for contract year 2014. Although we identified issues in contract years 2015 and 2016, they did not result in a penalty due to OPM or a credit due to the plan.

Specifically, we found that the plan:

- Lacked strong internal controls and written policies over its capitation rate-setting and MLR reporting processes;
- Used an inconsistent approach to record FEHBP expenses in its general ledger;
- Was not in compliance with OPM's Claims Data Requirements Carrier Letter for contract years 2014 through 2016;
- Incorrectly allocated its Patient-Centered Outcome Research Institute fees in contract years 2014 through 2016;
- Did not maintain all supporting documentation for the FEHBP MLRs for 2014 through 2016; and
- Included inaccurate medical and capitation expenses in its 2014 MLR.

Aetna Open Access

Blue Bell, Pennsylvania
Report Number 1C-99-00-17-007
December 17, 2019

We performed a global audit of Aetna Open Access, covering nine plan codes. The audit covered contract year 2013. 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.

Specifically, we found that the plan:

- Did not have sufficient internal controls over the FEHBP MLR reporting process;
- Erred in the reporting of the quality health improvement expenses, pharmacy claims adjustments, capitation payments, vendor payments, non-income tax expenses, and membership due to the weak control environment;
- Paid claims for unsupported dependent members over the age of 26;
- Paid claims for non-covered benefits; and
- Was not in compliance with OPM's Claims Data Requirements Carrier Letter for contract year 2013.

We also found that OPM's Community-Rating Guidelines do not sufficiently address the impact of corporate structure on the reporting of FEHBP MLR income tax expenses. Since Federal and State income taxes, which are material adjustments to the denominator of the MLR, could not be determined, we were unable to provide an opinion on the MLR as a whole for these nine plan codes. We are addressing these and other MLR administration issues with OPM through other channels.

Experience-Rated Carriers

The FEHBP offers a variety of experience-rated plans, including a service benefit plan, indemnity 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.

During the current reporting period, we issued seven final audit reports on experience-rated health plans participating in the FEHBP. These seven final audit reports contained recommendations for the return of over $11 million to the OPM-administered trust fund.

BlueCross BlueShield Service Benefit Plan Audits

The BlueCross BlueShield Association (BCBS Association), on behalf of 64 participating plans offered by 36 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 the BCBS Service Benefit Plan.

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, located in Washington, D.C. 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 summaries of three recent BCBS audits that are representative of our work.

BlueCross BlueShield of Vermont

Montpelier, Vermont
Report Number 1A-10-28-19-011
November 19, 2019

Our audit of the FEHBP operations at BCBS of Vermont (BCBS of VT) covered health benefit payments and credits (such as refunds and provider audit recoveries) from January 2015 through September 2018, as well as administrative expense charges from 2015 through 2017. We also reviewed the BCBS of VT's cash management activities and practices related to FEHBP funds from 2017 through September 2018.

We questioned $55,319 in net administrative expense overcharges, cash management activities, and lost investment income. The BCBS Association and BCBS of VT agreed with all of the questioned amounts.

Specifically, our audit identified the following:

- There were no findings pertaining to miscellaneous health benefit payments and credits. Overall, we concluded that BCBS of VT timely returned health benefit refunds and recoveries to the FEHBP and properly charged miscellaneous payments to the FEHBP.
- We questioned $52,665 in net administrative expense overcharges consisting of $63,715 for unallocable costs, $2,520 for net executive compensation overcharges, $19,917 for net Affordable Care Act fee undercharges, and $6,347 for lost investment income on the questioned overcharges.
- The plan held excess FEHBP funds of $2,654 in the dedicated Federal Employee Program investment account as of September 30, 2018. These excess funds were for provider overpayment recoveries that were deposited into the dedicated investment account but not returned to the FEHBP.

We verified that BCBS of VT subsequently returned all questioned amounts to the FEHBP.

BlueCross BlueShield of Arizona

Phoenix, Arizona
Report Number 1A-10-56-19-009
January 22, 2020

Our audit of the FEHBP operations at BCBS of Arizona (BCBS of AZ) covered miscellaneous health benefit payments and credits from 2014 through September 2018, as well as administrative expense charges from 2013 through 2017. We also reviewed the BCBS of AZ's cash management activities and practices related to FEHBP funds from 2014 through September 2018, and the plan's fraud and abuse program activities from January 2018 through December 2018.

We questioned $373,623 in miscellaneous health benefit credits, administrative expense charges, and lost investment income. The BCBS Association and BCBS of AZ agreed with all of the questioned amounts. As part of our review, we verified that BCBS of AZ subsequently returned these questioned amounts to the FEHBP.

Our audit results are summarized as follows:

- We questioned $31,624 for miscellaneous income and $24,664 for special plan invoice amounts that had not been returned to the FEHBP and $3,704 for lost investment income on these questioned amounts. The questioned special plan invoice amounts were for member overpayments that were several years old. BCBS of AZ decided to hold the members harmless for these overpayments and reimburse the FEHBP from corporate funds.
- We questioned $287,563 for quality improvement cost overcharges and $26,068 for lost investment income on these overcharges.
- There were no findings pertaining to BCBS of AZ's cash management activities and practices. Overall, we determined that BCBS of AZ handled FEHBP funds in accordance with the contract and applicable laws and regulations.
- There were no findings pertaining to the BCBS of AZ's fraud and abuse program activities. We concluded that BCBS of AZ is in compliance with the applicable communication and reporting requirements for fraud and abuse cases.

Claims Processing and Payment Operations at CareFirst BlueCross BlueShield

Owings Mills, Maryland
Report Number 1A-10-85-17-049
October 23, 2019. Reissued April 15, 2020

The audit's objectives were to determine whether CareFirst BCBS charged costs to the FEHBP and provided services to FEHBP members

in accordance with the terms of the BCBS Association's contract with OPM. Specifically, our objective was to determine whether the plan complied with the contract provisions relative to health benefit payments.

Our audit identified $3,058,657 in health benefit overcharges.

We found that CareFirst BCBS:

- Incorrectly paid 5,119 claims, totaling $1,227,289 in overcharges to the FEHBP, due to billing an incorrect place of service, which also potentially resulted in duplicate payments.
- Incorrectly paid 45 claims, totaling $1,364,155 in overcharges to the FEHBP as part of our system pricing, contract, and license review. In most instances, these errors were due to payments made to non-licensed preferred provider organization (PPO) overseas providers.
- Incorrectly paid 119 claims, totaling $467,213 in overcharges to the FEHBP as part of our amounts paid greater than or equal to billed charges review. In most instances, these errors were due to payments made to non-licensed PPO overseas providers.

Of the 10 audit recommendations included in this report, one has been closed, four have been resolved, and five remain open. Of the $3,058,657 questioned, $117,320 has been returned, $18,609 was allowed as uncollectible claims, $1,695,439 is being contested by the plan, and the remaining $1,227,289 is in the process of being recovered.

Global Audits

Global audits of BCBS plans are cross-cutting reviews of specific issues that we determine are likely to cause improper payments. These audits cover all 64 BCBS plans offered by the 36 participating BCBS companies.

We issued one global audit report related to experience-rated health plans during the reporting period, which is summarized below.

Claim Amounts Paid that Equaled or Exceeded Covered Charges at all BlueCross BlueShield Plans

This Audit fieldwork was conducted in Washington, D.C.
Report Number 1A-99-00-18-005
March 13, 2020

The audit's objectives were to determine whether the BCBS plans charged costs to the FEHBP and provided services to FEHBP members in accordance with the terms of the BCBS Association's contract with OPM. Specifically, our objective was to determine whether the plans complied with the contract provisions relative to claims where the amounts paid were equal to or exceeded covered charges.

Our audit identified $7,015,173 in health benefit overcharges.

We found that the plans incorrectly paid 396 claims for a variety of reasons, including manual overrides of claims that the claims processing system deferred for closer review. We also discovered that the system did not properly defer claims when billed charges were less than contractual rates, or when the system incorrectly applied pricing allowances. Other payment errors were related to provider billing errors, incorrect contract rates, and coordination of benefits with other insurers.

The audit also identified a program improvement area related to reimbursing non-participating providers at a more reasonable rate in lieu of billed charges. To OPM's credit, it revised the FEHBP's 2019 outpatient non-par (non-par means 'non-participating' provider, those that do not have a provider agreement or contract with the plan) non-emergency benefit structure to limit non-participating provider payments to the lesser

of the local plan allowance or the billed charges. This revision mitigated a large portion of this program concern; however, the change did not address the non-par emergency claims, which plans are still paying at billed charges. The biggest hurdle OPM faces in correcting this issue is the impact to the member.

The BCBS Association agreed with most of the audit recommendations and is working to provide OPM with a corrective action plan. All six audit recommendations remain open at this time.

Information Systems Audits

OPM manages a wide portfolio of information systems to help fulfill its mission. Although the Defense Counterintelligence Security Agency (DCSA) now administers the background investigations program for the Federal Government, OPM continues to operate the systems that support this program. OPM systems also support the processing of retirement claims and multiple Government-wide human resources services.

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 (IT) 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 and the 75 information systems used by private sector entities that contract with OPM to process Federal data. We issued eight IT system audit reports during the reporting period, and selected notable reports are summarized below.

The U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative

Washington, D.C.
Report Number 4A-CI-00-19-008
October 23, 2019

Our primary objective was to evaluate OPM's compliance and reporting for the Federal Information Technology Reform Act's Data Center Optimization Initiative (DCOI) requirements. In conjunction with this audit, we also reviewed the information technology security controls and documentation for OPM's three general support systems. Our audit determined that:

Data Center Optimization Initiative

OPM has defined a DCOI Strategic Plan to consolidate its data center infrastructure, including closing data centers. However, this plan has not been updated since 2017 and does not address any of the other DCOI objectives or targets.

While OPM has closed several data centers according to its plan, the agency has not implemented the required tools to optimize its remaining data centers. These include automated tools for monitoring, inventory, management, and power metering.

OPM has submitted the quarterly reports to the Office of Management and Budget (OMB), as required. However, some data elements from the reports are incorrect, including the number, closure status, and power utilization of the agency's data centers.

General Support System Security Controls

Our review of the system security documentation for each of the general support systems identified numerous issues. OPM policy does not define the documents that need to be updated and reviewed when an official in the assessment process leaves the agency. Additionally, there are issues with

the categorization, privacy assessments, risk assessments, weakness tracking, and security plans.

All three general support system data center spaces have physical access and physical environment vulnerabilities.

Federal Information Security Modernization Act Audit for Fiscal Year 2019

Washington, D.C.
Report Number 4A-CI-00-19-029
October 29, 2019

The Fiscal Year (FY) 2019 Federal Information Security Modernization Act (FISMA) Inspector General reporting metrics use a maturity model evaluation system derived from the National Institute of Standards and Technology's Cybersecurity Framework. The Cybersecurity Framework is comprised of eight "domain" areas, and the modes (i.e., the number that appears most often) of the domain scores are used to derive the agency's overall cybersecurity score. In FY 2019, OPM's cybersecurity maturity level was measured as "2 - Defined." While continued maturity is necessary, OPM made progress in FY 2019, closing several prior recommendations.

The following sections provide a high-level outline of OPM's performance in each of the eight domains from the five cybersecurity framework function areas:

Risk Management: OPM defined an enterprise-wide risk management strategy through its risk management council. OPM is working to implement a comprehensive inventory management process for its system interconnections, hardware assets, and software.

Configuration Management: OPM continues to develop baseline configurations and approve standard configuration settings for its information systems. The organization is also working to establish routine audit processes to ensure that its systems maintain compliance with established configurations.

Identity, Credential, and Access Management (ICAM): OPM is continuing to develop its agency ICAM strategy and acknowledges a need to implement an ICAM program. However, OPM still does not have sufficient processes in place to manage contractors in its environment.

Data Protection and Privacy: OPM has implemented some controls related to data protection and privacy. However, there are still resource constraints with OPM's Office of Privacy and Information Management that limit its effectiveness.

Security Training: OPM has implemented an IT security training strategy and program and performed a workforce assessment, but the agency still needs to identify gaps in its IT security training needs.

Information Security Continuous Monitoring (ISCM): OPM has established many of the policies and procedures surrounding ISCM, but the organization has not completed the implementation and enforcement of the policies. OPM also continues to struggle with conducting a security controls assessment on all of its information systems. Routine controls testing has been an ongoing weakness at OPM for over a decade.

Incident Response: OPM has implemented many of the required controls for incident response. Based upon our audit work, OPM has successfully implemented all of the FISMA metrics at the level of "consistently implemented" or higher.

Contingency Planning: OPM has not implemented several of the FISMA

requirements related to contingency planning, and the agency continues to struggle with maintaining its contingency plans and conducting contingency plan tests on a routine basis. Plan testing has been an ongoing weakness at OPM for over a decade.

Information Systems General and Application Controls at BlueCross BlueShield of Florida, Inc.
Jacksonville, Florida
Report Number 1A-10-41-19-028
February 13, 2020

Our IT audit focused on the claims processing applications used to adjudicate FEHBP claims for BlueCross BlueShield of Florida (BCBS of FL), Inc., BCBS of FL members, as well as the various processes and IT systems used to support these applications. Our audit of the IT security controls of BCBS of FL determined that the plan has an adequate IT security management program and controls over access to its facilities, network resources, and applications. The plan also has adequate contingency planning and controls over its claims adjudication system.

OPM'S CYBERSECURITY PROGRAM

In the FY 2019 Senate Appropriations Committee Financial Services and General Government Appropriations Bill Report, S. Rept. 115-281, the Committee 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, multi-factor authentication, and continuous monitoring; OPM's oversight of contractors providing IT services; and OPM's compliance with Government-wide initiatives to improve cybersecurity.[1] The following is a discussion of the above summary.

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 is still striving to define its IT enterprise architecture. Failure to have a defined IT enterprise architecture increases the risk that the agency's security processes, systems, and personnel are not aligned with the agency mission and strategic plan.

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.

OPM has enforced multi-factor authentication for non-privileged users for network and remote access using personal identity verification (PIV) cards. However, it has not configured multi-factor authentication for all major systems. Enforcing the use of PIV authentication for the network is not sufficient, as users or attackers that do gain access to the network can still access most

[1] Financial Services and General Government Appropriations Bill Report, S. Rept. 115-281.

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 PIV card. OPM has noted that it cannot fully implement multi-factor authentication because many of its legacy applications do not support the technology. This situation further demonstrates the importance of OPM's IT Modernization Plan.

OPM has developed an information security continuous monitoring (ISCM) strategy that addresses the monitoring of security controls at the organization, business unit, and individual information system level. However, in practice, OPM is not consistently implementing its ISCM strategy and has not met its objective of providing stakeholders with sufficient information to evaluate risks, primarily because OPM has not fully staffed its information system security positions. In FY 2019, only 8 of OPM's 47 systems were subject to adequate security controls testing and monitoring. The FY 2020 FISMA audit, which is currently in progress, will provide a current assessment of OPM's ISCM process and be discussed in a future semiannual report.

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.

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 OPM 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's operations and their corresponding internal controls. Our auditors are also responsible for conducting or overseeing certain statutorily required audits, such as 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 following summaries highlight notable audit findings from these audits.

OPM's Human Resources Staffing and Classification Process

Washington, D.C.
Report Number 4A-ES-00-18-049
October 2, 2019

Our auditors completed a performance audit of OPM's Human Resources Staffing and Classification processes. The Human Resources Staffing and Classification office's primary mission is to address all related human resources requirements for OPM personnel. This includes staffing, classification and consulting services, as well as developing solutions to complex classification human resources operational problems. Specific goals include: providing timely processing of new Federal employees through all human resources related areas; classifying proper position descriptions; creating appropriate job announcements; conducting job analyses; determining pay settings and leave; and validating applicant selections.

The objectives of our audit were to determine if OPM's Human Resources Staffing and Classification office is (1) following documented hiring processes, (2) meeting OPM's End-to-End Hiring Initiative timeliness best practices, (3) processing personnel actions in compliance with The Guide to Processing Personnel Actions, and (4) ensuring Human Resources Staffing and Classification employees are properly trained to perform their duties.

We determined that OPM's Human Resources Staffing and Classification office correctly processed personnel actions in compliance with The Guide to Processing Personnel Actions. However, we identified two areas where OPM should strengthen controls over its hiring processes and training for Human Resources Staffing and Classification employees. Specifically:

- The Human Resources Staffing and Classification office lacks proper documentation to verify that all 18 of its human resources specialists received the appropriate training to perform their job functions.
- We analyzed 42 new hire recruitment actions occurring between October 1, 2017, and September 30, 2018, and determined that 26 of the 42 new hire recruitment actions were not properly documented during the hiring process. In addition, 22 of the 42 new hire recruitment actions were not completed within the 80-day model, also known as OPM's End-to-End Hiring Initiative.

OPM's Oversight of the ID Experts Credit Monitoring and Identity Theft Services Contract

Washington, D.C.
Report Number 4A-OO-00-18-006
October 11, 2019

In FY 2015, OPM experienced two separate cyber-attacks that affected personnel records and background investigation records. Personally identifiable information (such as full names, birth

dates, home addresses, and Social Security numbers) of current, former, and prospective Federal Government employees, contractors, and others were stolen in these cyber-attacks on OPM systems.

OPM discovered the personal data of 4.2 million current and former Federal Government employees was stolen. In addition, OPM also discovered that 21.5 million background investigation records of current, former, and prospective Federal employees and contractors was stolen. Before the original contracts to provide identity theft protection and credit monitoring services to the affected individuals expired, a new contract was awarded to ID Experts on December 21, 2018.

ID Experts is responsible for providing various services to individuals affected by both the personnel records and background investigation records incidents. The services included in the two original contracts, which ended on December 31, 2018, are also included in the current contract, which ends on June 30, 2024.

The objectives of our performance audit were to determine if (1) the Contracting Officer's Representative (COR) is monitoring the contractor's performance in accordance with the Federal Acquisition Regulation and OPM's policies and procedures; and (2) Identity Theft Guard Solutions LLC, conducting business as ID Experts, and its subcontractor, Experian, are performing their duties and responsibilities in accordance with contract requirements.

Our auditors determined that ID Experts and Experian are performing their duties and responsibilities in accordance with contract requirements. However, we identified one area in which OPM should improve its controls over contract oversight.

The COR did not perform all duties as outlined by OPM's policies and procedures for monitoring the ID Experts contract. Specifically:

- Records (e.g., Memoranda for the Record) covering all meetings or discussions between the COR and the contractor were not prepared and maintained.
- The COR did not conduct any site visits to the contractor's facility to check the contractor's performance.
- The COR did not document reviews of the performance reports submitted by the contractor. In addition, the COR did not request supporting documentation to validate the data reported in the contractor's reports.

OPM's Data Submission and Compliance with the Digital Accountability and Transparency Act of 2014

Washington, D.C.
Report Number 4A-CF-00-19-025
November 6, 2019

The Digital Accountability and Transparency Act (DATA Act) of 2014 was enacted on May 9, 2014, to expand the reporting requirements pursuant to the Federal Funding Accountability and Transparency Act of 2006. The DATA Act, in part, requires Federal agencies to report financial and award data in accordance with the established Government-wide financial data standards. In May 2015, OMB and Treasury published 57 data definition standards and required Federal agencies to report financial and award data in accordance with these standards for DATA Act reporting, beginning in January 2017. Beginning in May 2017, in accordance with the DATA Act, Treasury began displaying Federal agencies' data on USASpending.gov so that taxpayers and policymakers could review and use the information.

The objectives of our audit were to assess (1) the completeness, accuracy, timeliness, and quality of FY 2019, first quarter, financial and award data submitted for publication on USASpending.gov; and (2) OPM's implementation and use of the Government-wide financial data standards established by OMB and Treasury.

We found that OPM's first quarter FY 2019 financial and award data submitted for publication on USASpending.gov was complete, accurate, and timely. Specifically, the following error rates, which we identified and projected to the population, comply with DATA Act reporting requirements.

Component	Error Rate	Margin of Error
Completeness	11.2%	2.5%
Accuracy	12.6%	2.6%
Timeliness	9.7%	2.5%

With respect to the overall data quality, OPM's data is classified as being in the higher category, because the highest error rate of 12.6 percent is less than 20 percent, as prescribed in the DATA Act Compliance Guide. OPM effectively implemented and used the Government-wide financial data standards established by OMB and Treasury.

We also identified one area where OPM needs to strengthen controls over its DATA Act submission process to ensure that no discrepancies exist in the linkages between Files C and D1. Specifically, 23 out of 199 transactions tested were identified in File C (award financial) and not in File D1 (award procurement).

OPM concurred with our findings and will make corrective actions.

OPM'S CONSOLIDATED FINANCIAL STATEMENTS AUDITS

The Chief Financial Officers Act of 1990 requires that audits of OPM's financial statements be conducted in accordance with Government Auditing Standards issued by the Comptroller General of the United States. OPM contracted with Grant Thornton LLP, an independent certified public accounting firm, to audit the consolidated financial statements as of September 30, 2019, and for the FY then ended. The contract requires that the audit be performed in accordance with generally accepted Government auditing standards (GAGAS) and OMB Bulletin No. 19-03, Audit Requirements for Federal Financial Statements.

OPM's consolidated financial statements include the agency's Retirement Program, Health Benefits Program, Life Insurance Program, Revolving Fund Programs, and Salaries and Expenses funds. The Revolving Fund Programs provide funding for a variety of human resource-related services to other Federal agencies, such as pre-employment testing and employee training. The Salaries and Expenses Funds provide the resources used by OPM for the administrative costs of the agency.

Grant Thornton is responsible for, but is not limited to, issuing an audit report that includes:

- Opinions on the consolidated financial statements and the individual statements for the three benefit programs;
- A report on internal controls; and
- A report on compliance with certain laws and regulations.

In connection with the audit contract, we oversee Grant Thornton's performance of the audit to ensure that it is conducted in accordance with the terms of the contract and complies with GAGAS and other authoritative references. Specifically, we

were involved in the planning, performance, and reporting phases of the audit through participation in key meetings, reviewing Grant Thornton's work papers, and coordinating the issuance of audit reports. Our review disclosed no instances where Grant Thornton did not comply in all material respects with GAGAS.

OPM's FY 2019 Consolidated Financial Statements

Washington, D.C.
Report Number 4A-CF-00-19-022
November 15, 2019

Grant Thornton audited OPM's consolidated financial statements, which comprise of the consolidated balance sheets as of September 30, 2019 and 2018, the related consolidated statements of net cost, changes in net position, and the combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements (collectively, the" financial statements"). Grant Thornton also audited the individual balance sheets of the Retirement, Health Benefits, and Life Insurance programs (hereafter referred to as the Programs), as of September 30, 2019 and 2018, the Programs' related individual financial statements of net cost, changes in net position, and budgetary resources for the years then ended, and the related notes to the individual financial statements.

Grant Thornton reported that OPM's consolidated financial statements and the Programs' individual financial statements as of and for the years ended September 30, 2019 and 2018, were presented fairly, in all material respects, and in conformity with U.S. Generally Accepted Accounting Principles. Grant Thornton's audits generally include identifying internal control deficiencies, significant deficiencies, and material weaknesses.

An **internal control deficiency** exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

A **significant deficiency** is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

A **material weakness** is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis.

Grant Thornton identified one material weakness in the internal controls related to OPM's information systems control environment, but they did not identify any significant deficiencies.

Information Systems Control Environment

During FY 2019, deficiencies noted in FY 2018 continued to exist, and Grant Thornton's testing identified similar control issues in both design and operation of key controls. These deficiencies continue to exist because of one, or a combination, of the following:

- Lack of centralized or comprehensive policies and procedures;
- The design of enhanced or newly designed controls did not completely address risks and recommendations provided over past audits;
- Oversight and governance was insufficient to enforce policies and address deficiencies; and/or
- Risk mitigation strategies and related control enhancements require additional time to be

fully implemented or to effectuate throughout the environment.

The information system issues identified in FY 2019 included repetitive conditions consistent with prior years as well as new deficiencies. The deficiencies in OPM's information systems control environment are in the areas of Security Management, Logical Access, Configuration Management and Interface/Data Transmission Controls, and, in the aggregate, are considered to be a material weakness.

OPM concurred with the findings and recommendations reported by Grant Thornton. Grant Thornton's report also identified instances of non-compliance with the Federal Financial Management Improvement Act of 1996 (FFMIA) Section 803(a), as described in the material weakness, in which OPM's financial management systems did not substantially comply with the Federal financial management systems requirements. The results of Grant Thornton's tests of FFMIA Section 803(a) disclosed no instances of substantial noncompliance with the applicable Federal accounting standards and the application of the United States Government Standard General Ledger at the transaction level.

Special Audits

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

- Federal Employees' Group Life Insurance (FEGLI) Program,
- Federal Flexible Spending Account (FSAFEDS) Program,
- Federal Long Term Care Insurance Program (FLTCIP), and
- Federal Employees Dental and Vision Insurance Program (FEDVIP).

Our office also conducts audits of Pharmacy Benefit Managers (PBMs) that administer pharmacy benefits for the FEHBP carriers. The objective of these audits is to ensure costs charged and services provided to Federal subscribers are in accordance with the contracts and applicable Federal regulations. Our staff also performs audits of the Combined Federal Campaign to ensure monies donated by Federal employees and annuitants are properly handled and disbursed to charities according to the designations of contributing employees, as well as audits of tribal enrollments into the FEHBP.

The following report was issued during this reporting period.

Management Advisory Report
Federal Employees Health Benefits Program
Prescription Drug Benefit Costs
Washington, D.C.
Report Number 1H-01-00-18-039
Original Report Issue Date: February 27, 2020
Corrected Report Issue Date: March 31, 2020

The primary purpose of this Management Advisory Report is to inform OPM of concerns that the OIG has regarding the escalating cost of the prescription drug benefit in the FEHBP.

It is vital OPM explore all possible methods to lower the cost of the prescription drug benefits in the FEHBP. The OIG has identified the rising costs of prescription drugs in its "Top Management Challenges" reports annually issued to OPM. Prescription drug benefits are a major component of the cost for the FEHBP, currently representing over 27 percent of total premiums spent on drugs, net of member cost share. Considering prescription drug spending in the United States is about 17 percent of overall personal health care expenditures, there may be an opportunity to reduce the drug spend in the FEHBP. Most FEHBP carriers report an increase in drug costs per member each year. Greater utilization of existing drugs and the expanding costs of specialty drugs contribute significantly to FEHBP premiums.

For decades now, pharmacy benefits have been provided by the majority of participating FEHBP carriers through contracts with PBMs. Instead of capitalizing on the purchasing power of over 8 million FEHBP members to generate greater savings, each of the hundreds of FEHBP carriers separately contract with a PBM, sometimes with less negotiating leverage than other health carriers, resulting in FEHBP pharmacy costs that vary greatly.

The FEHBP was established 60 years ago and remains the single largest employer-sponsored health care program in the United States. During this period, the founding principles in which OPM uses to guide its administration of the FEHBP has not changed. In fact, the FEHB Act still precludes OPM from contracting or negotiating with PBMs directly;

therefore, OPM must rely on contracted carriers to negotiate PBM drug discounts, rebates, and other benefits on behalf of the FEHBP. This can result in a lack of controls and the stagnation of any program modernization. OPM should research whether taking control and condensing FEHBP prescription drug benefit components would produce an overall strategy that reduces benefit costs.

Our concern remains that OPM may not be obtaining the most cost effective pharmacy benefits under the FEHBP. We believe OPM should consider all possible options to gain additional savings and maximize cost containment efforts, starting by conducting an independent study.

ENFORCEMENT ACTIVITIES

Investigative Activities

The mission of the Office of Investigations is to protect from fraud, waste, and abuse current Federal employees, annuitants, and their eligible beneficiaries who rely on OPM programs, as well as to safeguard 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), the FEHBP, and FEGLI—amount to over $1 trillion. These programs cover more than 8 million current and retired Federal civilian employees and eligible family members and annually disburse more than $140 billion in benefits.

Our Office of Investigations conducts criminal, civil, and administrative investigations of fraud, waste, abuse, and mismanagement related to OPM programs and operations. Our work prioritizes investigations into allegations of harm against those reliant on OPM programs such as the FEHBP and Retirement Services (Federal retirement and insurance programs); allegations causing substantial losses of taxpayer dollars; and agency program weaknesses that allow fraud, waste, and abuse.

Our priority investigations in the fight against the opioid epidemic target the crisis at all its levels, including pharmaceutical companies that prioritize profits over patient safety, unsafe or unscrupulous sober homes operating as places of patient harm instead of as places of recovery, or unethical physicians or pharmacists who prioritize profits over patient health. We continue to operate in partnerships with other agencies and law enforcement organizations nationwide in this ongoing fight.

Our investigative activities help return taxpayer dollars improperly paid. We also identify program vulnerabilities so that OPM can institute program-level changes to protect Federal employees, annuitants, and their eligible dependents. This remains a priority of the Office of Investigations in line with the President's Management Agenda goal to reduce improper payments.

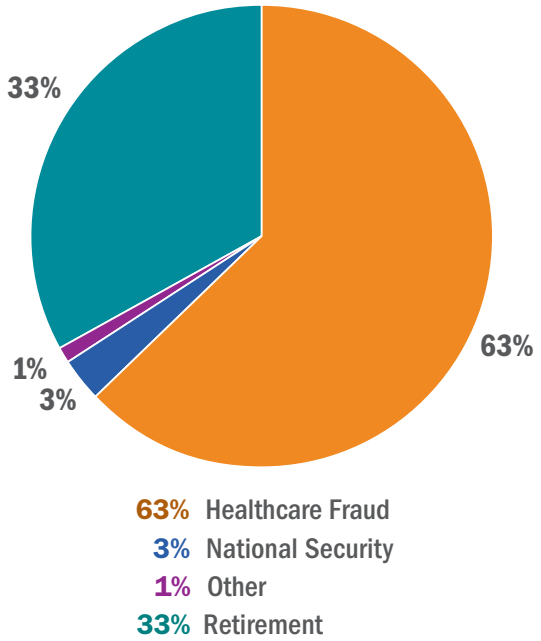
OPM reported total payments exceeding $55 billion ($48.56 billion in premiums to experience-rated carriers and $6.52 billion in premiums to community-rated carriers) related to the FEHBP and $80.65 billion in defined benefits related to OPM's Retirement Services office in FY 2019.[2] In FY 2019, OPM paid more than $339 million in improper payments from OPM-administered programs.[3] This $339 million in improper payments is a small portion of the total

[2] OPM Agency Financial Report Fiscal Year 2019 (127–128).

[3] Id. at. 127.

annual expenditures of the FEHBP and Federal retirement programs, but it is a total potentially undercounted per identified fraud trends by both of our Offices of Audits and Investigations. In its response to the OIG's FY 2020 Top Management Challenges report, OPM stated it is currently reviewing some of its improper payment rate methodologies (specifically related to the FEHBP), and we continue to engage with the agency in our shared goal to reduce fraud, waste, or abuse and to prevent and recover improper payments.[4]

Enforcement Actions by Case Type



During this reporting period, our investigative efforts led to 27 arrests, 23 indictments and criminal informations (an indictment is presented by a grand jury; a criminal information is presented by a duly authorized public official), and 26 convictions during this reporting period. We also took part in actions that resulted in $3,799,195 in monetary recoveries to OPM-administered trust funds. Many of our investigations are conducted jointly with other law enforcement agencies, and we actively coordinate with the U.S. Department of Justice (DOJ) and other Federal, State, and local law enforcement authorities. Criminal, civil, and administrative recoveries and fines returned to the General Fund of the Treasury totaled $27,817,733. For a statistical summary of Office of Investigations' investigative activities and financial recoveries, refer to page 40.

Below, we provide an overview of our investigative priorities and observed trends in fraud, waste, and abuse. We also provide case summaries representative of the Office of Investigations' diligent work to protect OPM, OPM programs, and beneficiaries. 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:

23 Indictments and Criminal Informations

27 Arrests

26 Convictions

And the Recovery to OPM of Over

$3.7 Million

[4] Id. at 123.

THE 2019 NOVEL CORONAVIRUS

The 2019 novel coronavirus (COVID-19) pandemic represents a fast-changing and extraordinary health care environment. OPM and the FEHBP health insurance carriers are communicating and working together during this health care crisis. On March 11, 2020, the OPM Healthcare and Insurance program office released FEHBP Carrier Letter 2020-02 to provide information to FEHBP health insurance carriers and to request alterations in coverage that would improve access and lower costs to FEHBP enrollees who contract COVID-19.

The OIG is committed to taking all necessary actions to protect Federal employees, annuitants, and their eligible dependents and the FEHBP from those who would take advantage of the ongoing pandemic. We are especially monitoring for potential instances of fraud, waste, and abuse that may negatively affect the health and safety of the Government's first responders and those Federal employees working against the pandemic on behalf of the public, many of whom are FEHBP enrollees, and we are especially vigilant regarding schemes that may affect these commendable individuals.

Like the opioid crisis, opportunistic criminals will use the COVID-19 pandemic for their own benefit; already, fake coronavirus tests have been intercepted nationwide. U.S. Attorney General William P. Barr released a memorandum to U.S. Attorneys regarding the potential for fraud and created a Hoarding and Price Gouging Task Force, and the General Services Administration posted warnings related to COVID-19 fraud and price gouging.[5] We anticipate the possibility of unethical providers promoting COVID-19 cures, treatments, or vaccines in schemes that could affect FEHBP enrollees or other OPM program beneficiaries.

We are also monitoring the pandemic response for any other health care fraud schemes or criminal trends that could worsen or more significantly affect the FEHBP because of the various shelter-in-place and stay-at-home orders across the country. For example, the National Institutes of Health's National Institute on Drug Abuse and the Substance Abuse and Mental Health Services Administration released pandemic-specific information noting that those battling addiction may be at greater risk of complications from COVID-19 and discussing the negative effects of isolation on these populations.[6] We are, in particular, watching substance abuse and recovery fraud as a potential ancillary fraud trend. And while various health agencies have promoted telehealth providers as necessary deliverers of care during the crisis, we remain watchful to ensure that telemedicine is conducted with the safety of FEHBP enrollees and the integrity of the FEHBP intact.

While no cases reported in this semiannual report to Congress directly engage with the pandemic, our Office of Investigations anticipates fraud, waste, and abuse related to the pandemic can and will emerge, and we are taking proactive steps to protect the FEHBP enrollees.

THE OPIOID EPIDEMIC

The opioid crisis remains a public health emergency.

Since October 26, 2017, when President Donald J. Trump declared the opioid and drug abuse crisis a public health emergency, thousands of Americans have died. The U.S. Department of Health and Human Services renewed its public health emergency declaration nine times.

---

[5] https://www.justice.gov/coronavirus; https://interact.gsa.gov/blog/important-covid-19-fraud-and-price-gouging

[6] https://www.drugabuse.gov/related-topics/covid-19-resources; https://www.samhsa.gov/sites/default/files/virtual-recovery-resources.pdf

However, statistics and provisional data show that the crisis, particularly as it relates to opioid-related overdoses, is slowing. The U.S. Centers for Disease Control and Prevention reported modest declines in opioid-related overdoses between 2017 and 2018. In such a complex crisis, many factors and actions contribute to these encouraging trends—including the combined efforts of the Government to increase access to treatment and recovery, as well as law enforcement efforts, like ours, to target those at any level of the health care system who illegally and cruelly contribute to the crisis.

Through our law enforcement actions, we protect Federal employees, retirees, and their eligible family members by investigating opioid-related cases at every level of the crisis:

Manufacturing Level Abuse: Some drug manufacturers and pharmaceutical companies encourage the proliferation of drugs of abuse and attempt to exploit the health care system for financial gain, often at the risk of patient harm.

Prescriber Level Abuse: Unethical doctors prescribe opioids and other potentially abused drugs without establishing medical relationships, determining medical necessity, or following appropriate prescribing guidelines.

Patient Level Abuse: Patients shop doctors to maintain a supply for their addiction or sell medications that supply those suffering from addiction.

Treatment Level Abuse: Disreputable sober homes and recovery centers exploit patients seeking treatment, often through unnecessary and inflated drug testing or the creation of sober homes that allow drug abuse, relapse, and patient harm.

In this semiannual report, we share the following opioid-related representative cases and updates to previously reported cases in prior reports:

First Prosecution of Opioid Manufacturer Leads to Prison Sentences, Additional Cases

In our last semiannual report to Congress, we reported our involvement in the landmark case charging Insys Therapeutics executives with various crimes, including operating in violation of the Racketeer Influenced and Corrupt Organizations Act.[7] In addition to the founder and former chairman being convicted, four other Insys executives were convicted in May 2019. The case is the first successful prosecution of pharmaceutical executives as part of the opioid crisis.

On January 23, 2020, Insys Therapeutics' founder and former board chair was sentenced to 66 months in prison for his role in Insys' scheme to bribe health care providers to prescribe a fentanyl-based medication. This is the first high-ranking pharmaceutical executive convicted and sentenced to a substantial term of imprisonment for actions contributing to the opioid crisis.

In addition to the main case against Insys Therapeutics, we joined a related case in the U.S. District Court for the Southern District of New York against five providers alleged to be participating in a kickback and bribery scheme that paid sham educational programs in exchange for prescribing millions of dollars of a fentanyl-based opioid. Among these five providers, the FEHBP had more than $63,000 in exposure. All five of the providers were referred to our FEHBP Administrative Sanctions Group for proposed debarment from the FEHBP.

Between February 2019 and August 2019, four of the five providers pled guilty to violating the Anti-Kickback Statute (AKS). One was sentenced to two years in prison and two years of supervised release, as well as ordered by the court to a forfeiture of $127,100. In December 2019, a Federal

[7] https://www.opm.gov/news/reports-publications/semi-annual-reports/sar61.pdf

jury found one provider guilty on one count of conspiracy to violate the AKS, one count of violating the AKS, and one count of conspiracy to commit honest services wire fraud. On January 27, 2020, one individual was sentenced to 57 months of imprisonment and 3 years of supervised release. The court also ordered forfeiture of $68,400 and a restitution order is pending.

Provider Pleads Guilty to 42-Count Indictment

In April 2016, we participated with law enforcement partners in a strike force investigating allegations that a provider billed patients for identical orders of compounded drugs and ran a pill mill that cost the FEHBP more than $319,000 in false claims and all other insurance programs involved more than $3.2 million in false insurance claims. The provider was arrested in June 2019. On January 24, 2020, the provider pled guilty in the U.S. District Court for the Eastern District of Pennsylvania to a 42-count indictment: 19 counts of health care fraud and 23 counts of distribution of Schedule II and Schedule IV controlled substances. The provider admitted to submitting nearly $10 million in false insurance claims, selling opioid medications to pill-seeking patients, and providing "goodie bags" containing medically unnecessary prescription drugs, including Schedule IV controlled substances.

Pennsylvania Pharmacist Sentenced to 36 Months Imprisonment for Opioid-Related Health Care Fraud

We presented a criminal case for prosecution to the U.S. Attorney's Office in the Eastern District of Pennsylvania regarding a pharmacist potentially overly dispensing Schedule II drugs based on data from the Pennsylvania Prescription Monitoring Program. Specifically, we became aware of the case because of a nurse under investigation by local law enforcement for inappropriately dispensing Schedule II drugs on more than 20 occasions.

During our investigation, the pharmacist involved admitted to defrauding health insurance carriers by billing for services not rendered via a coupon card program (submitting claims for name-brand drugs but dispensing less expensive generics) and creating fake prescriptions. The FEHBP paid $300,326 in claims to the pharmacy.

In April 2019, the nurse was charged for filling fraudulent prescriptions, including those for opioids. She pled guilty in the U.S. District Court for the Eastern District of Pennsylvania in May 2019 to conspiring to distribute oxycodone.

In September 2019, the pharmacist entered a guilty plea in the U.S. District Court for the Eastern District of Pennsylvania for conspiracy to commit wire fraud and 14 counts of prescribing medications outside the course of professional practice and not for legitimate medical purpose, including Schedule II controlled substances (including opioids). On March 12, 2020, the pharmacist was sentenced to 36 months in prison and 24 months of supervised release. The court ordered $300,000 in civil restitution, of which the FEHBP will receive $45,373. Additionally, the court ordered the provider to pay criminal restitution of $1.69 million to one pharmaceutical company.

OFFICE OF INVESTIGATIONS HEALTH CARE INVESTIGATIONS

The FEHBP is the largest employer-sponsored health insurance program in the world, covering about 8.2 million Federal current civilian employees, retirees, and their eligible family members. The program receives overall positive ratings from enrollees for program satisfaction in its annual member surveys. However, the program is susceptible to fraud, waste, and abuse—both from any programmatic weaknesses within the FEHBP and from the same fraud, waste, and abuse that affects the health care system at large.

Approximately 80 percent of the criminal cases that the OIG investigates involve health care fraud.

In FY 2019, OPM made $54.94 million in identified improper payments by the FEHBP. Without oversight and the work of the Office of Investigations, both patients and the FEHBP program are at risk.

Health Care Fraud and FEHBP Improper Payments

The health care fraud, waste, and abuse we investigated during this semiannual reporting period continues to be a mix of familiar crimes, many of which are now facilitated by recent technological developments. Bad providers, drug manufacturers, and fraudsters use important innovations, such as telemedicine, to their own avaricious ends—sometimes at the expense of patient health. We work diligently to investigate and resolve cases across the health care spectrum.

We continue to use data-driven methodologies to identify potential fraud, and we engage in various partnerships to increase the reach of the Office of Investigations and better protect FEHBP enrollees and the program. This includes our ongoing participation in nationwide law enforcement task forces and cooperation with the Federal Bureau of Investigation (FBI), DOJ, and others. We also participate in public-private partnerships such as the Health Care Fraud Prevention Partnership. One of our most significant cooperative efforts is the large-scale engagement with the health insurance carriers that partner with the FEHBP to provide health insurance coverage. As required by the FEHBP Carrier Letter 2013-17, those insurance companies provide carrier notifications that can alert our office to potential fraud, waste, abuse, or patient harm.[8]

Some of our investigations into potentially significant or viable cases end without recoveries to OPM programs because of the FEHBP's continued statutory exclusion from the AKS. While the Government may still partially recoup funds through investigations by other agencies, losses caused because of FEHBP exposure can result in thousands, and in some instances, millions of dollars being excluded as damages or absent from restitution orders.

HEALTH CARE FRAUD INVESTIGATIONS

In this semiannual reporting period, the following are some cases representative of our health care fraud investigations:

Compounding Pharmacy Provider Ordered to Pay $1.7 Million in Restitution

We received an allegation from the FBI that a provider for a specialty compounding pharmacy committed health care fraud by inducing doctors to sign blank prescriptions for compounded drugs without a medically necessary reason and billed these prescriptions to insurers at inflated rates. A sales representative for the compounding pharmacy received commissions as high as 17 percent of the cost of these unnecessary compounded prescriptions.

The FEHBP paid more than $1 million to one of the doctors who received the inducements. The total amount of FEHBP funds improperly paid based on the marketer's involvement is unknown, but the total loss to all programs—including the FEHBP, TRICARE, and others—is estimated at more than $9 million.

In July 2017, the marketer was charged with conspiracy to commit health care fraud, violations of the Travel Act, wire fraud, and violations of the AKS. These charges also supported that the marketer forged prescriptions in addition to the inducement scheme. In February 2019, the marketer pled guilty

[8] See the OIG Investigative Case Activity table on page 40 for detailed statistics regarding carrier notifications and program office referrals.

to conspiracy to commit wire fraud, health care fraud, violations of the Texas Commercial Bribery Statute, and the payment of health care bribes and kickbacks. On January 16, 2020, the marketer was sentenced to 30 months of imprisonment and 3 years of supervised release. The court also ordered the marketer to pay $1.74 million in restitution, of which $48,109 is owed to the FEHBP.

DOJ Employee Who Added Ineligible Beneficiaries to Their FEHBP Plan Pleads Guilty

In July 2017, we received a referral from the U.S. Attorney's Office in the Northern District of Texas alleging that a DOJ employee added multiple ineligible beneficiaries to her FEHBP health insurance plan. These ineligible beneficiaries were a friend and that friend's four children. The FEHBP paid more than $12,000 for services to the five ineligible beneficiaries. In February 2018, the DOJ employee and her friend were indicted on two counts of false statements related to health care matters, as well as aiding and abetting. In July 2018, the DOJ employee pled guilty and in April 2018, she was sentenced to 3 years of probation. She was ordered to pay restitution of $12,316 to the FEHBP. In March 2020, the friend who was added as an ineligible beneficiary pled guilty in the U.S. District Court for the Northern District of Texas for theft in connection with health care matters.

Compounding Scheme Costs the FEHBP More Than $2.3 Million

We received a referral from a law enforcement partner regarding a compounding pharmacy engaged in a fraud and inducements scheme that cost the FEHBP more than $2.3 million. In September 2019, a pharmacist and a marketer associated with the pharmacy were indicted in the U.S. District Court for the Central District of California on charges of conspiracy to commit mail fraud, wire fraud, health care fraud, aggravated identity theft, payment of illegal remunerations, conspiracy to commit money laundering, aiding and abetting, and criminal forfeiture. On October 22, 2019, the marketer pled guilty to illegal remunerations and criminal forfeiture.

RETIREMENT ANNUITY FRAUD INVESTIGATIONS

CSRS and FERS provide benefits for nearly 2.7 million Federal retirees and survivor annuitants receiving monthly annuity payments. Our Office of Investigations works to safeguard this program and those who rely on it through its investigations into allegations of identity theft, theft of Government funds, and other crimes—some of which are forms of elder abuse that take advantage of the aging population of Federal retirees.

Many of the cases we investigate are cases where the fraud is undiscovered for years and the cost to the OPM Federal retirement programs is in the tens of thousands of dollars. These types of frauds usually center on the forging of Address Verification Letters and other correspondence that OPM uses to verify the retiree annuitant rolls.

During this reporting period, members of our Investigative Support Operations group (ISOG) and our criminal investigative staff met with OPM regarding potential improvements to the Retirement Services' customer service, including its online services. We provided insight into potential factors for fraud, waste, and abuse based on existing fraud trends we observed in annuity-related fraud cases. We look forward to working with both OPM's Office of the Chief Information Officer and the Retirement Services office to provide oversight and feedback to reduce the potential for annuity theft and other crimes affecting Federal retirees and their families.

Our ISOG also uses proactive data analysis to identify fraud, waste, and abuse in the CSRS and

FERS programs. This process can generate leads for our criminal investigators, and even in the event the cases do not generate potential criminal cases, these proactive identifications are able to uncover funds that can be recovered through the Department of the Treasury's (Treasury) reclamation process.

The Office of Investigations is also prepared to use the Representative Payee Fraud Prevention Act of 2019, signed into law by President Donald J. Trump on March 18, 2020, to protect FERS and CSRS retirees whose annuities may be stolen or misused by Representative Payees. Under the previous legal framework, we were unable to pursue many investigations. In one such recent case, a nursing home provider contacted us and alleged that a Federal annuitant's brother stole the annuity and caused the annuitant to accumulate substantial unpaid debts and to be subsequently evicted from the nursing home. After the death of the annuitant four months later, the brother also unsuccessfully attempted to collect on the Federal annuitant's life insurance policy. We were unable to pursue a criminal case in the matter. In the future, with the Representative Payee Fraud Prevention Act of 2019, we hope to be able to devote more of our resources to investigating cases of this nature and better protecting Federal annuitants.

Proactive Projects and Recoveries

Below, we highlight selected cases representative of our investigations related to fraud, waste, and abuse in the Federal retirement annuity programs:

Our proactive recoveries, primarily the result of the work of our ISOG, are largely generated by projects which evaluate sets of annuitants in order to reduce fraud, waste, and abuse. Most of these cases are related to the types of retirement annuities that generated years of improper payments. Past and ongoing projects have involved reviewing cases of older annuitants on OPM annuity rolls who have a Representative Payee, as well as annuitants with suspended annuities but whom OPM Retirement Services has not confirmed to be alive, and others.

Our proactive projects recovered more than $1.06 million during this 6-month semiannual reporting period through criminal restitution orders, the Treasury's reclamation process, and voluntary repayment agreements.

Deceased Annuitant's Death Hidden in Annuity Theft

Our proactive review of Federal annuitants over the age of 90 with no health care claims in 10 years found an annuitant who continued to receive an annuity from OPM; however, our criminal investigators were unable to locate or contact the annuitant. A review of his beneficiary forms revealed suspicious and possibly forged signatures. Our investigation identified a potential suspect who lived at the same location as the annuitant. According to information presented to the U.S. District Court for the Eastern District of Michigan, the suspect forged several signatures on documents in order to steal the Federal retiree's annuity.

In the course of our investigation, the suspect admitted the annuitant died in early 2005. Since that time, the suspect received more than $800,000 in benefits from Government programs, including $566,000 in fraudulently received OPM annuity payments. The actual location of the annuitant's body remains unknown.

In August 2019, the suspect pled guilty to mail fraud and aggravated identity theft, which carries a mandatory minimum sentence of 2 years imprisonment. On December 3, 2019, the suspect was sentenced in the U.S. District Court for the Eastern District of Michigan to 2 years of incarceration (receiving only 1 day for the theft of Government funds) and 36 months of probation.

The court also ordered restitution of $566,000 to OPM stolen in the annuity theft.

Proactive Work Leads to Full Restitution

Our ISOG proactively identified an annuitant whose death was unreported to OPM's Retirement Services office. The annuitant died in May 2006, but Retirement Services continued to make payments for 12 years, until May 2018. The improper payment totaled $77,231. Reclamation actions by the Treasury recovered $21,440. The case was declined for prosecution in the U.S. District Court for the Eastern District of Michigan. However, the subject of the investigation contacted our criminal investigator and requested information on reimbursing the improper payment. On December 5, 2019, Retirement Services received a check for the remaining due balance of $55,790.

Annuity Thief Sentenced to 18 Months of Imprisonment

We received a referral from Retirement Services alleging OPM had not received timely notification of an annuitant's December 2001 death. Retirement Services continued to pay the CSRS survivor annuity payments through September 2016 for a total improper payment exceeding $123,000. Our investigation uncovered that the annuitant's daughter stole the annuity for her own use. In December 2018, she was indicted in the U.S District Court for the Central District of California on eight counts of mail fraud, eight counts of theft of Government property, and one count of aggravated identity theft. In April 2019, she pled guilty to mail fraud. On December 9, 2019, she was sentenced to 18 months in prison, 2 years of supervised release, and was ordered to pay restitution of $121,985 to OPM and $155,079 to another Federal retirement program.

Annuity Diverted for 22 Years Ends in Plea Agreement

We received a case referral from Retirement Services' Retirement Inspections group regarding an annuitant whose death in April 1995 was not reported to OPM. Annuity payments continued until September 2017. According to Retirement Services' records, the improper payments cost the CSRS program $404,112 in losses over 22 years. However, the bank where the annuity was deposited only kept records for seven years, which showed CSRS payments totaling more than $107,000.

Our investigation found the account that received the direct deposit was accessible by the annuitant's son, who died in 2012, and another individual. This individual converted the annuity for her own use. In August 2019, she was indicted in the U.S. District Court for the Eastern District of Missouri on charges of theft of Government funds. On January 8, 2020, she pled guilty to the charge. Sentencing and restitution are scheduled for a later date.

IMPACT TO NATIONAL SECURITY

The Office of Investigations provided oversight to OPM's National Background Investigations Bureau (NBIB), which conducted 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 pursued 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.

This semiannual reporting period is the first since the role formerly performed by NBIB was transferred to the Department of Defense (DoD) and its duties are no longer carried out as a bureau of OPM. However, our Office of Investigations continued its law enforcement efforts related to specific legacy cases involving the alleged fabrication of background investigations begun prior to NBIB's transition to becoming DoD's Defense Counterintelligence and Security Agency (DCSA) on October 1, 2019.

Our special agents provided assistance to DoD as the transition occurred so that its oversight offices are prepared to inherit the types of cases that our criminal investigators were charged with investigating.

In March 2020, we entered into an interagency agreement (Agreement) with DCSA to provide investigative services related to the legacy NBIB referrals to our office dated before October 1, 2019. Under this Agreement, our office invoices the DCSA for criminal investigative services performed by our office, after which DCSA non-criminal investigative staff determine the appropriateness of the invoice. Unlike other investigative activities our Office of Investigations conducts, our investigations of these fabrication cases do not return funds to OPM's Revolving Fund directly through the recoveries, restitution orders, fines, or other common means of recoupment. These are the only pay-for-service law enforcement functions that our Office of Investigations provides, and we are dependent on DCSA paying according to its evaluation of our costs.

INTEGRITY INVESTIGATIONS

A fundamental purpose of our Office of Investigations is to provide objective oversight and investigate allegations of fraud, waste, and abuse against OPM-administered programs and misconduct by OPM employees or contractors. These civil, criminal, and administrative investigations of integrity-related matters ensure the public has full faith in the agency's execution of its public duties.

As per the Inspector General Act of 1978, as amended, our semiannual reports to Congress must include all integrity cases involving senior Government officials or whistleblower retaliation.

In this reporting period, we had no reportable integrity-related investigations and cases.

HOTLINE COMPLAINTS

The OIG's Fraud Hotline also contributes to identifying fraud, waste, and abuse. The Hotline telephone number and mailing address are listed on our website at https://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse, along with an online complaint form that allows the complainant to remain anonymous. Contact information for the Hotline is also published in the brochures for all of the FEHBP health insurance plans. Those who report information to our Hotline can do so openly, anonymously, and confidentially without fear of reprisal.

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

In this semiannual reporting period, we improved our Hotline reporting system through a partnership with a public university contracted to provide intake processing for incoming complaints. Similar university agreements provide hotline-related services for several other OIGs. Once fully implemented, this agreement will allow our ISOG to process viable hotline complaints more quickly and provide better oversight of OPM programs.

We received 1,092 hotline inquiries during the reporting period, and closed 419. The table on page 41 reports the summary of hotline activities received through telephone calls, emails, and letters.

Administrative Sanctions of FEHBP Health Care Providers

Under the FEHBP administrative sanctions authority (Title 5 United States Code § (U.S.C.) Section 8902a), we suspend or debar health care providers whose actions demonstrate they are not sufficiently professionally responsible to participate in the FEHBP. At the end of the reporting period, there were 36,558 active suspensions and debarments of health care providers participating in the FEHBP.

Debarment disqualifies a health care provider from receiving payment of FEHBP funds for a stated time period. 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 remains in effect 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.

During the reporting period, our office issued 334 administrative sanctions, including both suspensions and debarments, of health care providers who committed violations impacting the FEHBP and its enrollees. In addition, we responded to 2,152 sanctions-related inquiries.

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

- Administrative actions issued against health care providers by other Federal agencies;
- Cases referred by the OIG's Office of Investigations;
- Cases identified by our administrative sanctions team through systematic research and analysis of electronically available information about health care 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 the health and safety of 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.

Pennsylvania Physician and His Medical Practice Debarred after Losing Medical License for Operating Prescription Pill Mill

In October 2019, our office debarred a Pennsylvania physician and his practice after the Pennsylvania State Board of Medicine (Medical Board) suspended the physician's medical license along with any other licenses to practice his profession.

An affidavit was filed in October 2017 against this physician and his office manager for conspiring to illegally distribute controlled substances such as OxyContin, Percocet, and MS Contin.

This prescription pill mill took place at the physician's medical practice in Philadelphia, Pennsylvania where addicts and drug dealers obtained prescriptions from the physician for the controlled substances in exchange for cash. The prescriptions were knowingly and intentionally distributed without a legitimate medical purpose or a doctor/patient relationship. The physician's actions were outside the normal course of professional practice. Therefore, the Medical Board ordered the physician's medical license be immediately, but temporarily, suspended, along with any other license to practice his profession. Accordingly, the provider's licenses issued by the Drug Enforcement Administration and New Jersey State Board of Medicine were also suspended.

Both the physician and his practice where he carried out this illicit activity were debarred from participating in the FEHBP for an indefinite period pending the reinstatement of the physician's medical license(s). This case was referred to us by our Office of Investigations.

Maryland Physical Therapist and Facility Debarred Due to Denial of License Reinstatement

In December 2019, our office debarred from participating in the FEHBP a physical therapist based on the Maryland State Board of Physical Therapist (MD Board) decision to deny the reinstatement of his physical therapy license.

The MD Board received complaints about this physical therapist and its investigation revealed this individual:

- Had an inappropriate sexual relationship with a patient;
- Failed to appropriately document his treatment of this particular patient;
- Publicly posed and continued to practice as a physical therapist after his license had expired;
- Improperly billed for physical therapy services after his license had expired; and
- Falsified his application for reinstatement.

The MD Board found the physical therapist's actions were unprofessional in the practice of physical therapy. The MD Board also found the physical therapist displayed a lack of good moral character, a failure to respect the dignity of the patient, and caused unnecessary and unacceptable risk to the public. Therefore, in 2017, the MD Board denied the physical therapist's application for reinstatement of his physical therapy license.

Our office debarred the physical therapist for an indefinite period pending the reinstatement of his license. The physical therapy facility in which the debarred provider carried out his inappropriate and unprofessional behavior was formerly owned by the debarred physical therapist. Although the facility was no longer owned by the debarred physical therapist, it continued to operate under the expired physical therapist's license. Therefore, we also debarred the physical therapy facility from participating in the FEHBP for a term concurrent with the physical therapist's debarment. This case was referred to us by our Office of Investigations.

Two Missouri Surgical Facilities Debarred Due to Ownership by the Debarred Provider

Our office debarred two surgical facilities from participating in the FEHBP, one in January 2020 and one in March 2020, owned by a provider our office previously debarred for health care fraud. In January 2019, we debarred the owner of these facilities for a period of five years based on her 2018 conviction in the U.S. District Court for the Eastern District of Missouri, for making false statements relating to health care matters.

The surgeon pled guilty to submitting false claims to health care insurers for the reimbursement of medical services not provided. The surgeon did not provide the medical services to the patients listed on the billed submissions, nor did she have a valid medical license at the time the claims were submitted. The surgeon was sentenced to five years of probation and was ordered to pay $304,844 in restitution to health care insurers, of which approximately $64,067 is due to the FEHBP.

5 U.S.C. § 8902a(c)(2) provides OPM authority to debar an entity that is owned or controlled by an individual who is currently debarred, suspended, or otherwise excluded from any procurement or non-procurement activity. The regulations at Title 5 Code of Federal Regulations (CFR) § 890.1003 define "control" as constituting the direct or indirect ownership of 5 percent or more of an entity, or serving as an officer, director, or agent of an entity. Therefore, we debarred the two surgical facilities owned by the debarred provider. In accordance with 5 C.F.R. § 890.1018(a), the debarment of the two surgical facilities will run concurrent with the surgeon's five-year debarment period. This case was referred to us by our Office of Investigations.

New York Physician and Clinic Debarred for Professional Misconduct

In October 2019, our office debarred from participating in the FEHBP a New York physician for professional misconduct after his license was restricted by the New York State Board for Professional Medical Conduct (NY Board). The NY Board cited the physician for violating New York Public Health Law PBH-230-a, charging him with professional misconduct.

The physician was disciplined by the NY Board for nontherapeutic prescribing; failing to adequately document medical records; failing to adequately supervise subordinates; aiding and abetting the practice of medicine by an unlicensed person; failing to maintain patient confidentiality; delegating responsibilities to an unauthorized person; and failing to treat patients according to the general standard of care.

The NY Board's disciplinary order prohibits the physician from the following:

- The practice of medicine clinical or otherwise, except when it pertains to himself, his wife, or his child, and may only electronically prescribe non-controlled substances for himself, his wife, and his child;
- Ordering, prescribing, dispensing, and/or administering controlled substances or submitting claims to insurance carriers on behalf of himself, his wife, or his child; and
- Further reliance upon his New York State medical license to exempt him from the licensure, certification, or other requirements set forth in statute or regulation for the practice of any other profession licensed, regulated, or certified by the New York State Board of Regents, New York State Department of Education, New York State Department of Health or the New York State Department of State.

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

Our debarment of the physician is for an indefinite period pending full reinstatement of the physician's

medical license. This case was referred to us by an FEHBP carrier.

Kentucky Physician and Clinic Debarred, Florida Pharmacy and Owner Suspended for Involvement in Health Care Fraud

In November 2019, our office debarred from participating in the FEHBP a Kentucky physician based on the suspension of his license to practice medicine by the Commonwealth of Kentucky Board of Medical Licensure (KY Board). The KY Board issued the suspension after the physician was indicted in April 2019 in the U.S. District Court for the Western District of Kentucky for the following:

- Conspiracy to commit fraud;
- Offering or paying health care kickbacks;
- Health care fraud; and
- Health care fraud via inflated compounded drug prescriptions.

The indictment alleges the physician teamed up with a Florida pharmacy and its owner in a scheme that involved the payment of alleged kickbacks in return for writing prescriptions for compounded drugs that included controlled substances. The physician was also charged with fraudulently inflating the costs for prescriptions that were billed for reimbursement by Medicare and TRICARE.

The pharmacy owner was also indicted in April 2019 for his alleged role in illegally prescribing and distributing millions of pills containing opioids and other drugs. The physician and the pharmacy owner are both awaiting trial.

OPM may debar a health care entity based on an ownership or control interest by a debarred provider. In addition, OPM may immediately suspend a provider from participating in the FEHBP pending the completion of an investigation or ensuing criminal or administrative proceedings.

We debarred the physician and his clinic based on the loss of his medical license. Our debarment of the physician and clinic is for an indefinite period pending full reinstatement of the physician's medical license.

In addition, we suspended from participating in the FEHBP the pharmacy owner and the pharmacy involved in the illegal distribution of controlled substances. Suspension of the pharmacy owner and pharmacy will remain in place for an indefinite period pending formal entry of judgment. This case was referred to us by an FEHBP carrier.

EVALUATIONS 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 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. The Office of Evaluations 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. It is discussed below.

Presidential Rank Awards Program

Washington, D.C.
Report Number 4K-ES-00-19-032
January 15, 2020

Our analysts completed an evaluation during this reporting period of the Presidential Rank Awards Program. The Presidential Rank Award is one of the highest awards bestowed by the President of the United States upon the career Senior Executive Service and senior professionals who occupy Senior Level and Scientific or Professional positions. Within OPM, the Senior Executive Resources Services is responsible for administering the Presidential Rank Awards Program.

During our prior evaluation of OPM's Employee Services' Senior Executive Service and Performance Management Office, we learned about issues involving pending interagency agreements within the Presidential Rank Awards Program. As a result, we conducted this evaluation to determine whether OPM has effective controls in place to carry out its responsibilities with regard to managing and administering the Presidential Rank Awards Program.

We determined that the Senior Executive Resources Services needed to:

- Strengthen its controls over the Presidential Rank Awards Program. Specifically, management needed to:
  - Update and finalize its standard operating procedures to ensure Senior Executive Resources Services staff document required responsibilities and include instructions for processing interagency agreement obligation forms for on-site evaluation; and
  - Build on-going monitoring and quality control measures to ensure compliance.
- Work with the appropriate offices to close-out interagency agreements from FYs 2016, 2017, and 2018.

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

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

LEGAL AND LEGISLATIVE ACTIVITIES

Legislative Activities

Under the Inspector General Act of 1978, as amended, OIGs are required to obtain legal advice from a counsel reporting directly to an Inspector General. This reporting relationship ensures that the OIG receives independent and objective legal advice. The Office of Legal and Legislative Affairs discharges this statutory responsibility in several ways, including by providing advice to the Inspector General and the OIG office components on a variety of legal issues, tracking and commenting on legislative matters affecting the work of the OIG, and advancing legislative proposals which address waste, fraud, and abuse against and within OPM.

During this reporting period, the OIG provided technical comments to the House Committee on Oversight and Reform on the "Representative Payee Fraud Prevention Act of 2019," H.R. 5214, 116th Congress (2019). The legislation was introduced in November 2019 and enacted on March 18, 2020. Our Office of Legal and Legislative Affairs also negotiated the legal agreements which facilitated the continuity of our Office of Investigations' NBIB legacy oversight work within the newly-created DCSA.

New Legislation Introduces Important Protections for Vulnerable Federal Annuitants

As discussed in the IG Message, when a Federal employee retires, they are typically eligible to receive an annuity. These retirees (or in certain instances, their survivors) are referred to as annuitants. If an annuitant can no longer manage their own finances, OPM will appoint an individual to receive payments in their stead. These individuals, referred to as Representative Payees, often have close personal relationships (e.g., child, caretaker, or spouse) with the annuitant.

The Representative Payee Fraud Prevention Act of 2019 introduces several important protections for this vulnerable population. Signed by the President on March 18, 2020, the Act provides a clear definition of what constitutes fraud against a CSRS or FERS Federal annuitant – language which is useful for both deterring and prosecuting this crime. The Act also creates important bulwarks for preventing fraud against Representative Payees by codifying requirements that the agency act in the best interest of the Federal annuitant, ensuring that those who embezzle Federal annuity benefits are barred from serving as Representative Payees, and providing for the publication of agency regulations of the program.

Earlier iterations of this legislation were introduced in 2015 by Senators James Lankford (R-OK) and Heidi Heitkamp (D-ND) as well as in May 2019 by Senators Lankford, Gary Peters (D-MI), and Kyrsten Sinema (D-AZ). Both bills passed the Senate. The enacted version was introduced in the House by Representatives Rashida Tlaib (D-MI) and Mark Meadows (R-NC) in November 2019. Our Office of Legal and Legislative Affairs provided technical

assistance and background information on each version of the bill.

Ensuring the Integrity of Legacy Cases Involving the Former National Background Investigations Bureau

On October 1, 2019, OPM's NBIB officially transferred to DoD, as required by section 925 of the FY 2018 National Defense Authorization Act and Executive Order 13869, Transferring Responsibility for Background Investigations to DoD. Although NBIB has transitioned to what is now known as DCSA, the OPM OIG maintains responsibility for completing NBIB legacy oversight work, such as criminal investigations of alleged fabrication of background investigations opened prior to October 1, 2019. To ensure the continuity of the law enforcement investigations, our Office of Legal and Legislative Affairs worked to establish the necessary legal documentation (a memorandum of understanding and an inter-agency agreement) that provided the funding required for our Office of Investigations' criminal investigators to complete the NBIB legacy oversight work.

Statistical Summary of Enforcement Activities

Investigative Actions and Recoveries:

Indictments and Criminal Informations 23
Arrests 27
Convictions 26
Criminal Complaints/Pre-Trial Diversion 1
Subjects Presented for Prosecution 205
- Federal Venue 202
  - Criminal 39
  - Civil 163
- State Venue
  - Criminal 2
- Local Venue
  - Criminal 1

Expected Recovery Amount to OPM Programs $3,799,195
- Civil Judgments and Settlements $171,959
- Criminal Fines, Penalties, Assessments, and Forfeitures $2,409,830
- Administrative Recoveries $1,217,407

Expected Recovery Amount for All Programs and Victims[9] $27,817,734

Investigative Administrative Actions:

FY 2019 Investigative Reports Issued[10] 565

Whistleblower Retaliation Allegations Substantiated 0
Cases Referred for Suspension and Debarment 2
- Health Care Cases Referred to the OIG for Suspension and Debarment from the FEHBP 2
- NBIB Cases Referred to OPM for Suspension and Debarment of Contractors 0

[9] 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.

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

Personnel Suspensions and Terminations..... 0
Referral to the OIG's Office of Audits..... 0
Referral to OPM Program Office 1

Administrative Sanctions Activities:

FEHBP Debarments and Suspensions Issued..... 334
FEHBP Provider Debarment and Suspension Inquiries 2,152
FEHBP Debarments and Suspensions in Effect at the End of Reporting Period..... 36,558

OIG Investigative Case Activity

	Healthcare and Insurance	Retirement Services	Other OPM Program Offices	External/ Internal Matters	Total
Cases Opened	**219**	**34**	**14**	**9**	**276**
Investigations	2	1	0	0	3
Complaints	217	33	14	9	273
Inquiries Opened	**947**	**27**	**1**	**23**	**998**
Referrals – FEHBP Carriers/ Program Office	797	3	0	1	801
Referrals – All Other Sources/ Proactive	150	24	1	22	197
Cases Closed	**532**	**68**	**10**	**12**	**622**
Investigations	84	20	7	3	114
Complaints	448	48	3	9	508
Inquiries Closed[11]	**1,113**	**25**	**0**	**4**	**1,142**
Referrals – FEHBP Carriers/ Program Office	955	4	0	1	960
Referrals – All Other Sources/ Proactive	158	21	0	3	182
Cases In-Progress[12]	**484**	**70**	**41**	**13**	**608**
Investigations	155	37	7	5	204
Complaints	329	33	34	8	404
Inquiries In-Progress[13]	**201**	**2**	**0**	**2**	**205**
Referrals – FEHBP Carriers/ Program Office	199	0	0	0	199
Referrals – All Other Sources/ Proactive	2	2	0	2	6

[11] Cases closed may have opened in a previous reporting period.

[12] Cases in progress may have been opened in a previous reporting period.

[13] Inquiries in progress may have been opened in a previous reporting period.

OIG Hotline Case Activity

OIG Hotline Cases Received 1,092

Sources of OIG Hotline Cases Received

- Website 515
- Telephone 325
- Letter 107
- Email 145
- In-Person 0

By OPM Program Office

- Healthcare and Insurance 238
  - Customer Service 117
  - Billing Disputes 103
  - Other Healthcare and Insurance Issues 18
- Retirement Services 253
  - Customer Service 199
  - Annuity Calculation 31
  - Other Retirement Services Issues 23
- Other OPM Program Offices/Internal Matters 123
  - Customer Service 32
  - Other OPM Program/Internal Issues 83
  - Employee or Contractor Misconduct 8
- External Agency Issues (not OPM-related) 478

OIG Hotline Cases Reviewed and Closed 419

Outcome of OIG Hotline Cases Closed

- Referred to External Agencies 164
- Referred to OPM Program Office 150
  - Retirement Services 86
  - Healthcare and Insurance 55
  - Other OPM Programs/Internal Matters 9
- No Further Action 98
- Converted to a Case 7

OIG Hotline Cases Pending[14] 673

By OPM Program Office

Healthcare and Insurance 170
Retirement Services 153
Other OPM Program Offices/Internal Matters 104
External Agency Issues (not OPM related) 246

[14] Includes hotline cases pending an OIG internal review or an agency response to a referral.

APPENDICES

APPENDIX I

Final Reports Issued with Questioned Costs for Insurance Programs
October 1, 2019 – March 31, 2020

Subject		Number of Reports	Questioned Costs
A.	Reports for which no management decision had been made by the beginning of the reporting period	4	$84,027,268
B.	Reports issued during the reporting period with findings	8	$11,149,664
	Subtotals (A+B)	12	$95,176,932
C.	Reports for which a management decision was made during the reporting period:	6	$2,326,362
	1. Net disallowed costs	N/A	$116,700
	Disallowed costs during the reporting period	N/A	$2,214,357[1]
	Less: costs originally disallowed but subsequently allowed during the reporting period	N/A	$2,097,657[2]
	2. Net allowed costs	N/A	$2,209,662
	Allowed costs during the reporting period	N/A	$112,005[3]
	Plus: costs originally disallowed but subsequently allowed during the reporting period	N/A	$2,097,657
D.	Reports for which no management decision has been made by the end of the reporting period	6	$92,850,570
E.	Reports for which no management decision has been made within 6 months of issuance	3	$82,671,754

[1] Represents the management decision to support questioned costs and establish a receivable during the reporting period.

[2] Represents questioned costs which were determined by management to be allowable charges per the contract, subsequent to an initial management decision to disallow and establish a receivable. The receivable may have been set up in this period or previous reporting periods.

[3] Represents questioned costs (overpayments) which management allowed and for which no receivable was established. It also includes the allowance of underpayments to be returned to the carrier.

APPENDIX II

Resolution of Questioned Costs in Final Reports for Insurance Programs
October 1, 2019 – March 31, 2020

Subject		Questioned Costs
A.	Value of open recommendations at the beginning of the reporting period	$122,387,845
B.	Value of new audit recommendations issued during the reporting period	$11,149,664
	Subtotals (A+B)	$133,537,509
C.	Amounts recovered during the reporting period	$3,898,205
D.	Amounts allowed during the reporting period	$2,209,662
E.	Other adjustments	$0
	Subtotals (C+D+E)	$6,107,867
F.	Value of open recommendations at the end of the reporting period	$127,429,642

APPENDIX III

Final Reports Issued with Recommendations for Better Use of Funds
October 1, 2019 – March 31, 2020

Subject		Number of Reports	Dollar Value
A.	Reports issued during the reporting period with findings	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
October 1, 2019 – March 31, 2020

Report Number	Subject	Date Issued	Questioned Costs
1D-87-00-19-014	Claims Processing and Payment Operations at Hawaii Medical Service Association as a participating Health Maintenance Organization in Honolulu, Hawaii	October 15, 2019	$0
1A-10-85-17-049	Claims Processing and Payment Operations at CareFirst BlueCross BlueShield in Owings Mills, Maryland	October 23, 2019	$3,058,657
1C-NM-00-18-047	Health Plan of Nevada in Las Vegas, Nevada	November 14, 2019	$31,696
1A-10-28-19-011	BlueCross BlueShield of Vermont in Montpelier, Vermont	November 19, 2019	$55,319
1C-3A-00-18-052	AultCare Health Plan in Canton, Ohio	November 25, 2019	$0
1A-10-42-19-015	BlueCross BlueShield of Kansas City in Kansas City, Missouri	December 16, 2019	$168,660
1C-99-00-17-007	Aetna Open Access in Blue Bell, Pennsylvania	December 17, 2019	$0
1A-10-56-19-009	BlueCross BlueShield of Arizona in Phoenix, Arizona	January 22, 2020	$373,623
1A-10-47-19-013	Claims Processing and Payment Operations at Hawaii Medical Service Association as a participating Fee for Service Health Plan in Honolulu, Hawaii	January 24, 2020	$205,621
1A-99-00-18-005	Claim Amounts Paid that Equaled or Exceeded Covered Charges at all BlueCross BlueShield Plans in Washington, D.C.	March 13, 2020	$7,015,173
1C-SF-00-19-021	SelectHealth Inc. in Murray, Utah	March 27, 2020	$0
1A-10-41-16-029	Claims Processing and Payment Operations at BlueCross BlueShield of Florida in Jacksonville, Florida	March 30, 2020	$240,915
TOTAL			$11,149,664

APPENDIX V

Internal Audit Reports Issued
October 1, 2019 – March 31, 2020

Report Number	Subject	Date Issued
4A-ES-00-18-049	The U.S. Office of Personnel Management's Human Resources Staffing and Classification Process in Washington, D.C.	October 2, 2019
4A-OO-00-18-006	The U.S. Office of Personnel Management's Oversight of the ID Experts Credit Monitoring and Identity Theft Services Contract in Washington, D.C.	October 11, 2019
4A-CF-00-19-025	The U.S. Office of Personnel Management's Data Submission and Compliance with the Digital Accountability and Transparency Act of 2014 in Washington, D.C.	November 6, 2019
4A-CF-00-19-022	The U.S. Office of Personnel Management's Fiscal Year 2019 Consolidated Financial Statements in Washington, D.C.	November 18, 2019

APPENDIX VI

Information Systems Audit Reports Issued
October 1, 2019 – March 31, 2020

Report Number	Subject	Date Issued
4A-CF-00-19-026	Information Technology Security Controls of the U.S. Office of Personnel Management's Consolidated Business Information System in Washington, D.C.	October 3, 2019
4A-CF-00-19-027	Information Technology Security Controls of the U.S. Office of Personnel Management's Federal Financial System in Washington, D.C.	October 8, 2019
1A-10-40-19-010	Information Systems General and Application Controls at BlueCross BlueShield of Mississippi in Flowood, Mississippi	October 21, 2019
4A-CI-00-19-008	The U.S. Office of Personnel Management's Compliance with the Data Center Optimization Initiative in Washington, D.C.	October 23, 2019
4A-CI-00-19-029	Federal Information Security Modernization Act Audit Fiscal Year 2019 in Washington, D.C.	October 29, 2019
1C-P2-00-19-016	Information Systems General Controls at Presbyterian Health Plan in Albuquerque, New Mexico	November 18, 2019
1A-10-41-19-028	Information Systems General and Application Controls at BlueCross BlueShield of Florida, Inc. in Jacksonville, Florida	February 13, 2020
1C-22-00-19-020	Information Systems General and Application Controls at Aetna in Hartford, Connecticut	March 4, 2020

APPENDIX VII

Special Review Reports Issued
October 1, 2019 – March 31, 2020

Report Number	Subject	Date Issued
1H-01-00-18-039	Management Advisory Report - Federal Employees Health Benefits Program Prescription Drug Benefit Costs in Washington, D.C.	February 27, 2020 (Original) March 31, 2020 (Reissued)

APPENDIX VIII

Evaluation Reports Issued
October 1, 2019 – March 31, 2020

Report Number	Subject	Date Issued
4K-ES-00-19-032	Evaluation of the Presidential Rank Awards Program in Washington, D.C.	January 17, 2020

APPENDIX IX

Summary of Reports More Than Six Months Old Pending Corrective Action
As of March 31, 2020

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

Report Number	Subject	Date Issued	Recommendations	
			Open	Total
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, D.C.	March 23, 2015	2	3
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	Health Care 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

Report Number	Subject	Date Issued	Recommendations	
			Open	Total
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
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
IA-10-33-15-009	BlueCross BlueShield 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	14	19
4A-RS-00-16-035	Information Security Controls of the U.S. Office of Personnel Managements 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
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

Report Number	Subject	Date Issued	Recommendations	
			Open	Total
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	17	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	2	4
1A-99-00-16-021	Global Veterans Affairs Claims for BlueCross BlueShield 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	20	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

Report Number	Subject	Date Issued	Recommendations	
			Open	Total
1C-JK-00-18-029	TakeCare Insurance Company, Inc. in Tamuning, Guam	April 25, 2019	2	11
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	5	5
IA-10-32-18-046	Information Systems General and Application Controls at BlueCross BlueShield of Michigan in Detroit, Michigan	May 16, 2019	2	8
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	3	4
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	4	4
34A-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	5	5
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	6	13
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	5	6
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	3	5

APPENDIX X

Most Recent Peer Review Results
As of March 31, 2020

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 Special Inspector General for Afghanistan Reconstruction *(Issued by the Office of the Inspector General, U.S. Office of Personnel Management)*	March 10, 2020	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
External Peer Review Report on the Office of Evaluations of the Office of the Inspector General for the U.S. Office of Personnel Management *(Issued by the U.S. Consumer Product Safety Commission Office of Inspector General)*	December 16, 2019	Compliant[3]

[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 for the Office of Audits. 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.

[3] 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 for Inspections and Evaluations are followed.

APPENDIX XI

Investigative Recoveries
October 1, 2019 – March 31, 2020

Statistic Type	Program Office	Type of Recovery	Total Recovery Amount	Total OPM Net
Administrative			$2,519,998	$1,217,407
	Healthcare and Insurance		$1,485,019	$182,427
		Collection of Improper Payments	$50,825	$50,825
		Carrier Settlements	$1,434,194	$131,602
	National Background Investigations Bureau		$239,855	$239,855
		Contract Off-Sets	$239,855	$239,855
	Retirement Services		$795,124	$795,124
		Administrative Debt Recoveries	$303,709	$303,709
		Bank Reclamations	$940	$940
		Identification of Improper Payments	$434,685	$434,685
		Voluntary Payment Agreements	$55,791	$55,791
Civil			$19,102,778	$171,959
	Healthcare and Insurance		$19,102,778	$171,959
		Civil Actions	$19,102,778	$171,959
Criminal			$6,194,958	$2,409,830
	Healthcare and Insurance		$3,916,661	$693,035
		Court Assessments/Fees	$6,100	$0
		Criminal Fines	$250,000	$0
		Criminal Judgments/Restitution	$3,660,561	$693,035
	National Background Investigations Bureau		$212,032	$40,000
		Court Assessments/Fees	$2,200	$0
		Criminal Judgments/Restitution	$209,832	$40,000
	Retirement Services		$2,066,264	$1,676,795
		Court Assessments/Fees	$1,000	$0
		Criminal Judgments/Restitution	$2,065,264	$1,676,795
Grand Total			**$27,817,734**	**$3,799,195**

INDEX OF REPORTING REQUIREMENTS

(Inspector General Act of 1978, As Amended)

Section		Page
4(a)(2):	Review of legislation and regulations	37
5(a)(1):	Significant problems, abuses, and deficiencies	1–36
5(a)(2):	Recommendations regarding significant problems, abuses, and deficiencies	1–18, 35–36
5(a)(3):	Recommendations described in previous semiannual reports for which corrective action has not been completed	OIG's Website
5(a)(4):	Matters referred to prosecutive authorities	19-33, 39–42
5(a)(5):	Summary of instances where information was refused during this reporting period	No Activity
5(a)(6):	Listing of audit reports issued during this reporting period	45–47
5(a)(7):	Summary of particularly significant reports	1–18, 35–36
5(a)(8):	Audit reports containing questioned costs	43
5(a)(9):	Audit reports containing recommendations for better use of funds	44
5(a)(10):	Summary of unresolved audit reports issued prior to the beginning of this reporting period	48–52
5(a)(11):	Significant revised management decisions during this reporting period	No Activity
5(a)(12):	Significant management decisions with which the OIG disagreed during this reporting period	No Activity
5(a)(13):	Reportable information under section 804(b) of the Federal Financial Management Improvement Act of 1996	No Activity
5(a)(14):	Recent peer reviews of the OPM OIG conducted by other OIGs	53

5(a)(15): Outstanding recommendations from peer reviews of the OPM OIG conducted by other OIGs 53

5(a)(16): Peer reviews conducted by the OPM OIG 53

5(a)(17): Investigative statistics 39–40

5(a)(18): Metrics used for developing the data for the investigative statistics 39–40

5(a)(19): Investigations substantiating misconduct by a senior Government employee ..... No Activity

5(a)(20): Investigations involving whistleblower retaliation ..... No Activity

5(a)(21): Agency attempts to interfere with OIG independence ..... No Activity

5(a)(22)(A): Closed audits and evaluations not disclosed to the public ..... No Activity

5(a)(22)(B): Closed investigations not disclosed to the public 40–42

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/

March 2020
OIG–SAR–62

OVERSIGHT.GOV
ALL FEDERAL INSPECTOR GENERAL REPORTS IN ONE PLACE

Visit Oversight.gov to find reports from all Federal Inspectors General who are members of the Council of Inspectors General on Integrity and Efficiency (CIGIE).