



---

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

---

# Top Management Challenges: Fiscal Year 2020

**The U.S. Office of Personnel Management's  
Top Management Challenges for Fiscal Year 2020**

**November 6, 2019**

# EXECUTIVE SUMMARY

## *The U.S. Office of Personnel Management's Top Management Challenges for Fiscal Year 2020*

November 6, 2019

### **The Purpose of This Report.**

The Reports Consolidation Act of 2000 requires the Inspector General to identify and report annually the top management challenges facing the agency. We have classified the challenges into two key types of issues facing the U.S. Office of Personnel Management (OPM) – environmental challenges, which are either inherent to the program or function, or result mainly from factors external to OPM and may be long-term or even permanent; and internal challenges, which OPM has more control over and once fully addressed, will likely be removed as a management challenge.

### **What Did We Consider?**

We identified 13 issues as top challenges because they meet one or more of the following criteria: (1) the issue involves an operation that is critical to an OPM core mission; (2) there is a significant risk of fraud, waste, or abuse of OPM or other Government assets; (3) the issue involves significant strategic alliances with other agencies, the Office of Management and Budget, the Administration, Congress, or the public; (4) the issue is related to key initiatives of the President; or (5) the issue involves a legal or regulatory requirement not being met.



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

### **What Did We Find?**

The OIG identified the following four environmental challenges:

- Proposed OPM merger with the General Services Administration;
- Background Investigations;
- Strategic Human Capital Management; and
- Federal Health Insurance Initiatives.

These environmental challenges are due to external factors including, but not limited to, rapid technological advances, shifting demographics, various quality of life considerations, and national security threats that are prompting fundamental changes to Federal Government operations. Some of these challenges involve core functions of OPM that are affected by constantly changing ways of doing business or new ideas, while in other cases they are global challenges every agency must face.

The OIG also identified the following nine internal challenges:

- Information Security Governance;
- Information Security Continuous Monitoring;
- Data Security;
- Information Technology Infrastructure Improvement Project;
- National Background Investigations Bureau Legacy Information Systems;
- Stopping the Flow of Improper Payments;
- Retirement Claims Processing;
- Procurement Process Oversight; and
- Federal Employees Health Benefits Program Enrollment and Eligibility.

Information Security Governance is the only challenge currently reported as a material weakness in the fiscal year 2018 Federal Information Security Modernization Act (FISMA) report. While the remaining challenges are not currently considered material weaknesses in either FISMA or the Chief Financial Officers Act Financial Statement audit report, they are issues which demand significant attention, effort, and skill from OPM in order to be successfully addressed, or face the possibility of becoming material weaknesses and having a negative impact on OPM's performance if they are not handled appropriately by OPM management.

# ABBREVIATIONS

<b>CBIS</b>	<b>Consolidated Business Information System</b>
<b>DCSA</b>	<b>Defense Counterintelligence and Security Agency</b>
<b>DOD</b>	<b>Department of Defense</b>
<b>E.O.</b>	<b>Executive Order</b>
<b>EKRA</b>	<b>Eliminating Kickbacks in Recovery Act of 2018</b>
<b>FEHBP</b>	<b>Federal Employees Health Benefits Program</b>
<b>FISMA</b>	<b>Federal Information Security Modernization Act</b>
<b>FWA</b>	<b>Fraud, Waste, and Abuse</b>
<b>FY</b>	<b>Fiscal Year</b>
<b>GAO</b>	<b>U.S. Government Accountability Office</b>
<b>GSA</b>	<b>General Services Administration</b>
<b>HHS</b>	<b>U.S. Department of Health and Human Services</b>
<b>ISCM</b>	<b>Information Security Continuous Monitoring</b>
<b>IT</b>	<b>Information Technology</b>
<b>MLR</b>	<b>Medical Loss Ratio</b>
<b>NBIB</b>	<b>National Background Investigations Bureau</b>
<b>OCIO</b>	<b>Office of the Chief Information Officer</b>
<b>OIG</b>	<b>Office of the Inspector General</b>
<b>OMB</b>	<b>U.S. Office of Management and Budget</b>
<b>OPM</b>	<b>U.S. Office of Personnel Management</b>
<b>OPO</b>	<b>Office of Procurement Operations</b>
<b>PBM</b>	<b>Pharmacy Benefits Manager</b>
<b>PIV</b>	<b>Personal Identity Verification</b>
<b>PRISM</b>	<b>Procurement Information System for Management</b>

# TABLE OF CONTENTS

	<u>Page</u>
<b>EXECUTIVE SUMMARY</b> .....	i
<b>ABBREVIATIONS</b> .....	ii
<b>I. ENVIRONMENTAL CHALLENGES</b> .....	1
1. PROPOSED OPM MERGER WITH THE GENERAL SERVICES ADMINISTRATION .....	1
2. BACKGROUND INVESTIGATIONS .....	2
3. STRATEGIC HUMAN CAPITAL MANAGEMENT .....	4
4. FEDERAL HEALTH INSURANCE INITIATIVES .....	5
<b>II. INTERNAL CHALLENGES</b> .....	12
1. INFORMATION SECURITY GOVERNANCE .....	12
2. INFORMATION SECURITY CONTINUOUS MONITORING .....	13
3. DATA SECURITY .....	14
4. INFORMATION TECHNOLOGY INFRASTRUCTURE IMPROVEMENT PROJECT .....	15
5. NATIONAL BACKGROUND INVESTIGATIONS BUREAU LEGACY INFORMATION SYSTEMS .....	16
6. STOPPING THE FLOW OF IMPROPER PAYMENTS .....	17
7. RETIREMENT CLAIMS PROCESSING .....	18
8. PROCUREMENT PROCESS OVERSIGHT .....	20
9. FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM ENROLLMENT AND ELIGIBILITY .....	21
<b>REPORT FRAUD, WASTE, AND MISMANAGEMENT</b>	

# I. ENVIRONMENTAL CHALLENGES

The following challenges are issues that are potentially long-term challenges and could be on our list of top challenges for the U.S. Office of Personnel Management (OPM or “the agency”) for multiple years because of their dynamic, ever-evolving nature, and because they are mission-critical programs.

This fiscal year (FY) there is a change in the environmental top management challenges. Since the National Background Investigations Bureau (NBIB)<sup>1</sup> has transferred to the Department of Defense (DOD), the Case Processing Backlog is no longer a challenge for OPM and therefore has been dropped.

## 1. PROPOSED OPM MERGER WITH THE GENERAL SERVICES ADMINISTRATION (GSA)

In June 2018, the Executive Office of the President (or “the President” or “the Administration”) published *Delivering Government Solutions in the 21st Century: Reform Plan and Reorganization Recommendations*. The document puts forth a comprehensive plan that would reorganize OPM, including the transfer of a variety of OPM functions to the GSA. This proposal has also been set forth in the President’s most recent budget and a May 2019 formal legislative proposal submitted by the Administration to Congress. The legislative proposal would transfer the majority of OPM’s current functions and resources to GSA, including Human Resources Solutions, Information Technology (IT), Retirement, and the Healthcare and Insurance divisions. However, the proposal does not include a reorganization plan, shifting the burden to the agency to fully study, plan, and execute reorganization activities.

While the legislative proposal has not been introduced in either chamber of Congress, OPM continues to explore ways to merge functions with GSA, as demonstrated by the planned transfer of the Performance Accountability Council, Performance Management Office and Chief Human Capital Officers Council to GSA. Meanwhile, the specific details of the full OPM/GSA merger continue to evolve and every iteration of the proposed reorganization would fundamentally alter how agency functions and duties are performed. As directed by Congress and in accordance with authorities granted by the *Inspector General Act of 1978*, as amended, OPM’s Office of the Inspector General (OIG) has taken an active role in the oversight of the proposed OPM/GSA merger to confirm that the process is efficient, effective, and free of fraud, waste, and abuse.

---

<sup>1</sup> As of October 1, 2019, NBIB was transferred to DOD and is now known as the Defense Counterintelligence and Security Agency.

The agency appears to be aware of the inherent risks in the merger and has established decisional frameworks to monitor and discuss these risks. For example, OPM is using the “tollgate” process, a Six Sigma-based process used for mergers and acquisitions in the private sector, to steer the proposed reorganization plan. The agency has also attempted to engage employees by having the former Acting Director, Margaret Weichert, visit program offices. The former Acting Director participated in three town hall meetings focused on the reorganization; however, staff surveys have shown confusion and uncertainty related to the proposed merger. OPM leadership must continue to educate the staff on the reorganization in order to have an engaged and productive workforce.

The OPM OIG also remains concerned that many aspects of the proposed reorganization have not been fully documented. OPM lacks a developed analysis of alternative approaches to the merger, a thorough cost-benefit analysis, a comprehensive timeline, and documentation that delineates which legal or regulatory authorities OPM will use to administratively transfer agency functions. This is particularly evident with the planned transfer of the Performance Accountability Council, Performance Management Office and Chief Human Capital Officers Council. The agency has not conducted a business or cost-benefit analysis to justify the move of either Council. For example, the staff subject to the transition of the Chief Human Capital Officers Council to GSA would be appointed to new positions non-competitively once GSA cleared the positions through the Interagency Career Transition Assistance Plan. Not only does this process not guarantee current OPM staff reemployment at GSA, OPM has not conducted an assessment of the costs associated with this workforce restructuring. Until OPM undertakes the necessary planning to address these issues, the agency will encounter numerous challenges implementing the proposed reorganization.

In order to help ensure a successful outcome, OPM should conduct and fully document a thorough analysis of the options and the cost-benefit of those options. A review of published best practices for government reorganization may help with this effort. Beyond developing documentation to support the merger proposal, OPM leadership will also need to work towards acquiring buy-in by continuing to engage with a variety of stakeholders, including Congress, agency employees, and oversight bodies in the Executive and Legislative branches in order to effectively implement any full or partial reorganization. We look forward to continuing to work with the agency on the continued monitoring and review of these efforts.

## **2. BACKGROUND INVESTIGATIONS**

### **Transfer of the Background Investigation Function**

Following the massive data breach in 2015, the President issued an Executive Order (E.O.) to consolidate the background investigative services that OPM provides to Federal departments and agencies. In FY 2017, the National Defense Authorization Act directed the DOD to

prepare an implementation plan for the transfer of the background investigation responsibility for DOD-affiliated personnel from OPM to DOD. The plan proposed a three-year phased transition of the DOD-related investigations, which account for approximately 70 percent of NBIB's caseload. In December 2017, Section 925 of the FY 2018 National Defense Authorization Act directed DOD, in consultation with OPM, to begin carrying out the implementation plan no later than October 1, 2020, and authorized DOD to conduct background investigations for DOD-affiliated personnel. On April 24, 2019, the President signed E.O. 13869, *Transferring Responsibility for Background Investigations to the Department of Defense*, directing the transfer of the remaining non-DOD related investigations to DOD's newly created Defense Counterintelligence and Security Agency (DCSA). The E.O. stated that OPM delegate the authority to conduct these NBIB functions to DCSA, and required the transfer to DCSA take effect by October 1, 2019. The E.O. recognized that as part of this delegation, OPM would have a continuing role by establishing appropriate performance standards and oversight.

In response to the Congressional mandate to transfer DOD-related investigations, NBIB has undertaken numerous initiatives to address issues with the transfer, including identifying workforce processes, working capital and appropriated budgets, NBIB contracts, and the transfer of personnel from Title 5 to Title 10, as well as working with OPM's Office of the Chief Information Officer regarding strategies for legacy technology and NBIB data. In December 2018, NBIB published a backlog mitigation plan and reported a substantial decrease in the case backlog. We are also encouraged both by the dialogue between the two agencies, as well as by NBIB's efforts to thoroughly study and document this transfer. In June 2019, OPM delegated its authority to operate a clearance database and to conduct investigations to DOD. Over the course of FY 2019, NBIB made an effort to plan for an orderly transfer of the background investigation function.

The E.O. recognized, as mandated by Title 5, that OPM is required to establish appropriate performance standards and maintain an oversight program for this delegated authority to DOD. In addition, OPM may face a significant challenge regarding the transfer of IT systems to DCSA. OPM anticipates the transfer of IT systems to DCSA to take some time. In the interim, OPM will need to continue to maintain and secure OPM's legacy IT systems, which have presented challenges in the past. The OIG will monitor OPM's compliance with its legal requirements regarding the delegation and the transfer to DCSA, and the OIG will continue to monitor OPM's IT systems controls and legacy IT-related issues.

The E.O. also included the transfer of NBIB employees and resources associated with those functions from OPM to DOD. NBIB is the single largest component of OPM, employing approximately 3,000 full-time equivalent employees, and providing a variety of investigative products to over 100 federal agencies. Receipts for these services contribute over \$2.24

billion in revenue. Initially, the transfer of NBIB personnel and funds to DOD presented OPM with a \$70 million budget shortfall. Through OPM's successful advocacy with Congress and the Administration, the continuing resolution for FY 2020 included an additional \$48 million for OPM. Additionally, OPM anticipates partially mitigating the shortfall with the buyback by DOD of certain IT and financial services from OPM after the transfer. The OIG will continue to monitor how OPM plans to address funding of common services after the transfer of NBIB.

### **3. STRATEGIC HUMAN CAPITAL MANAGEMENT**

Since 2001, strategic human capital management has been on the U.S. Government Accountability Office's (GAO) high-risk list of Government-wide challenges requiring focused attention. In their March 2019 *HIGH-RISK SERIES Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas* report, GAO stated that over the years since this area was added to their high-risk list, in addition to recommendations to address critical skills gaps in individual high-risk areas, they have made numerous recommendations to OPM related to this high-risk issue, 29 of which remain open. Furthermore, GAO suggested that OPM fully address the open recommendations in its January 2015 report, which called on the Director of OPM to make more strategic use of government workforce data by building a predictive capacity for identifying and mitigating emerging skills gaps across Government. The report also recommended that OPM work with the Chief Human Capital Officers Council to bolster the ability of agencies to assess workforce competencies by sharing competency surveys, lessons learned, and other tools and resources.

#### **Skills Gaps Closure Progress**

Strategic human capital management remains high-risk because more work is needed to address Government-wide mission critical skills gaps. According to GAO's 2019 analysis of Federal high-risk areas, skills gaps played a role in approximately 49 percent of the Government-wide high-risk areas. Skills gaps within individual Federal agencies can lead to costly, less-efficient government.

In 2018, OPM reported that they worked with the Government-wide occupational leaders for the high risk Government-wide mission critical occupations of Auditor, Economist, Cybersecurity, Acquisition, and Human Resources Specialist. As a result, a new performance auditor standard has been approved and is being made 508 compliant for the Auditor occupation; a proposed regulation was drafted for a new pay system for the Economist occupation; the Cybersecurity Reskilling Academy was launched to fill cyber-related shortages; a partnership to increase efficiencies in current acquisition processes and practices was established with the George Washington University's Government



Procurement Law and Master of Science in Government Contracts programs for the Acquisition occupation; and a comprehensive suite of tools and training was developed for Human Resource professionals.

OPM also reported that in July 2019, they issued a data call to the Chief Human Capital Officers to collect additional information related to potential barriers and continued progress in mitigating gaps within their mission critical occupations. In addition, they are collaborating with GSA to find new methods to mitigate skills gaps. OPM is also working with agencies to assist with their reskilling and upskilling efforts and to conduct Strategic Workforce Foresight analysis to identify emerging and future workforce needs. Lastly, OPM conducted Human Capital Reviews with all 24 Chief Human Capital Officers agencies, meeting with their senior leadership, to support their human capital efforts and identify opportunities to mitigate skills gaps.

OPM should fully implement GAO's recommendations related to this high-risk area. In addition, they need to continue to develop resources and tools, facilitate best practices discussions, update and maintain its main domain (opm.gov), monitor the Government-wide Federal Action Skills Team action plans, pursue funding to ensure continuous development of Human Resources courses, and launch the Competency Exploration Development and Readiness (CEDAR) assessment tool to support agencies in identifying competency and skills gaps.

#### **4. FEDERAL HEALTH INSURANCE INITIATIVES**

A major, on-going challenge for OPM involves the Federal Employees Health Benefits Program (FEHBP). OPM must continue to administer a world-class health insurance program for Federal employees so that comprehensive health care benefits can be offered at a reasonable and sustainable price.

The following sections highlight these challenges and current initiatives in place to address them.

##### **Federal Employees Health Benefits Program**

As the administrator of the FEHBP, OPM has responsibility for negotiating contracts with insurance carriers covering the benefits provided and premium rates charged to over eight million Federal employees, retirees, and their families. The ever-increasing cost of health care, including the cost of prescription drugs, is a national challenge, affecting not only OPM. In 2019, OPM announced that the average premium increase for Federal employees and retirees participating in the FEHBP in 2020 would be 4 percent.

It is an ongoing challenge for OPM to keep these premium rate increases in check while not impacting the level of benefits offered. There are several initiatives that OPM is adopting to meet the challenge of providing quality health care for enrollees, while controlling costs. Examples include better analysis of the drivers of health care costs, purchasing of pharmacy benefits, and improved prevention of fraud and abuse.

Another major challenge for OPM is adjusting to changes in the health care industry's premium rating practices. In particular, the adoption of the Medical Loss Ratio (MLR) rating methodology requires that OPM update guidance and improve its financial reporting activities.

### **1) Prescription Drug Benefits and Costs**

Prescription drugs are a major share of health care costs in the FEHBP, currently representing approximately 27 percent of total health care expenditures. Most FEHBP carriers report an increase in drug costs per member each year. Greater utilization of existing drugs and the high cost of specialty medications contribute significantly to FEHBP premiums. Prescription drug utilization and costs will continue to increase for the foreseeable future, as new pharmaceutical advancements are developed and the rapid growth of the specialty drug market continues. OPM needs to develop an effective, long-term strategy to mitigate and manage FEHBP prescription drug costs, while maintaining overall program value and effectiveness.

Since the inception of the FEHBP, pharmacy benefits have been provided via participating FEHBP carriers by administering pharmacy benefits internally, or more often, by carriers contracting with a Pharmacy Benefits Manager (PBM) on behalf of their enrolled population. OPM has no involvement in negotiating drug discounts, rebates, administrative fees, or other financial terms with PBMs. FEHBP carriers are responsible for negotiating these contracts on behalf of the Federal Government. Furthermore, since OPM has minimal involvement in negotiating the contract terms between the individual carrier and the PBM, the fees (which are ultimately borne by the FEHBP) may not provide the best value to FEHBP members and the American taxpayer.

We believe the need for clear and extensive analysis of the FEHBP drug program cost-saving options is long overdue. The last time OPM formally studied the issue was approximately nine years ago. The PBM and prescription drug landscape has significantly changed since 2010. Our concerns about increasing prescription drug costs warrant the need to evaluate the benefits, delivery, and pricing of FEHBP prescription drugs specifically, including whether carrier PBM contracts provide the best value to the

Federal Government and FEHBP enrollees in today's environment. Moving forward, OPM needs to develop an effective, long-term strategy to mitigate and manage future FEHBP prescription drug costs, while maintaining overall program value and effectiveness. A focused independent study should be conducted to determine further prescription drug cost savings programs that could be implemented to help control future increases to the FEHBP.

## **2) Health Benefit Carriers' Fraud and Abuse Programs**

OPM's top challenges surrounding FEHBP fraud, waste, and abuse (FWA) programs are in part a result of the over-delegation of program integrity functions to carriers and the lack of adequate controls within OPM to support the program integrity of the FEHBP. To that end, the OIG continues to suggest Healthcare and Insurance establish a dedicated program integrity office, which has precedent elsewhere within the Federal healthcare program sector.

Both Medicare and TRICARE deploy comprehensive program integrity divisions to enhance and employ strategic oversight of FWA detection and prevention, program analytics, and trend analysis to enhance criminal, civil, and administrative enforcement efforts. For example, the U.S. Department of Health and Human Services OIG enforcement actions are increasingly data- and trend-driven, derived directly from their program integrity operations and initiatives through the Centers for Medicare & Medicaid Services.

OPM has shown it recognizes the importance of robust carrier FWA programs:

- In November 2017, Healthcare and Insurance issued Carrier Letter 2017-13 (CL 2017-13) to provide FEHBP carriers new guidance for reporting FWA.
- Healthcare and Insurance realigned its FWA team to analyze FEHBP carrier annual FWA reports to improve oversight.<sup>2</sup>

While CL 2017-13 yielded some improvement, Healthcare and Insurance cannot provide an effective measurement of the FWA program in the FEHBP. Local plan successes do not replace a full accounting or global measurement of efforts to reduce FWA within the FEHBP. There must be quantifiable standards of success, whether reductions in improper payments as identified by carrier fraud reports or other measures as determined by the agency.

---

<sup>2</sup> OPM FY 2018 Agency Financial Report, page 148.

The OIG remains concerned about subcontractors (in particular, PBMs and behavioral health subcontractors) whose FWA controls are layers removed from OPM oversight. Stronger program controls can help OPM recognize global fraud trends across the healthcare environment and support carriers with training and written guidance. Particularly, a permanent program integrity group dedicated to the assessment of FWA can provide consolidated approaches to analyze the effects of FWA, identify root causes, track improper payments, assess trends detected by carriers, and address programmatic issues contained in FWA reporting. Notwithstanding return on investment calculations, there is currently no all-encompassing effective measure of how well these FWA programs are working.

Additionally, a program integrity unit could help protect the FEHBP from global threats, such as the opioid crisis, by strengthening requirements for carrier internal control programs. For example, in 2018, Congress passed the Eliminating Kickbacks in Recovery Act of 2018 (EKRA). The law forbids kickbacks in one of the fastest increasing areas of FEHBP program fraud: recovery homes, clinical treatment facilities, and laboratories. However, there is no indication OPM is supporting, guiding, or working in conjunction with carriers to enhance fraud detection and reporting efforts related to EKRA.

The OIG is concerned the delegation of antifraud and program integrity functions beyond carriers and into multilayered environments of contractors and subcontractors (e.g., PBMs) has diluted OPM's ability to recognize and respond to global FWA trends affecting the FEHBP. A program integrity office dedicated to overseeing FWA programs, receiving carrier case notifications, tracking fraud trends and program vulnerabilities, and providing accurate data reporting would substantially improve OPM's ability to manage the program.

### **3) Medical Loss Ratio Oversight**

On June 29, 2011, OPM issued an interim final ruling replacing the Similarly Sized Subscriber Group methodology with an MLR calculation. The ruling holds each community-rated carrier, except those that are state-mandated to use traditional community rating, to a specific MLR, as determined by OPM. Simply put, community-rated carriers participating in the FEHBP must spend the majority of their FEHBP premiums on medical claims and approved quality health initiatives. If a carrier does not meet the MLR, it is required to pay a penalty amount to the FEHBP. If a carrier exceeds the MLR, it receives a credit from OPM that can be used to offset future penalties.

However, audits of the MLR calculation continue to identify concerns that question the validity of the data included in both the numerator and the denominator of this

calculation. Specifically, our audits identified the following concerns: the accuracy of OPM's subscription income amount; the carriers' ability to manipulate the MLR ratio (i.e., through claims and claim type costs, expense adjustments, etc.); and a continued lack of clear guidance from OPM to address issues specific to the FEHBP MLR calculation that cannot be addressed through the U.S. Department of Health and Human Services (HHS) guidance that OPM also uses for the FEHBP.

OPM states that it now has the ability to document and support the data included in the subscription income report. Specifically, by accessing the computer code in the program and having records to support the data, OPM states that the subscription income is now reliable. However, further review will need to occur before the OIG can state an opinion as to whether the subscription income report is a reliable source for the premium number used by most carriers in their MLR calculation.

OPM does not believe that carriers are overstating or manipulating their MLR calculations through allocations and other methods, such as capitation. Furthermore, OPM does not believe it is in the FEHBP's best interest to issue global guidance to address these types of concerns as it only impacts a small percentage of carriers. However, based on the results of our audits, we continue to find that allocations are being inconsistently and inequitably applied. Furthermore, capitation arrangements and the expenses paid to capitated providers are not clearly identifying and accounting for FEHBP member benefits and cost sharing payments, in conjunction with the community benefits in the development of the capitated rate or payment.

We agree that overly prescriptive MLR instructions may not be ideal and some flexibility in deriving MLR percentages should be granted to the carriers. However, the methodologies used in the MLR calculation need to be accurate, auditable, and consistently enforced. In instances where this is not the case and the resulting issues cannot be adequately addressed by the HHS guidelines, it is incumbent upon OPM to develop its own guidance to address these issues.

OPM states that it continues to review its MLR policies to provide more meaningful and clear guidance and is willing to discuss any issues with the OIG and other parties. We welcome this openness and encourage OPM to continue to assess and update their guidance as issues become known in order to ensure reliable MLR calculations.

#### **4) The Opioid Epidemic and the FEHBP**

The President's 2017 memorandum, *Combating the National Drug and Opioid Crisis*, specified that agencies "shall exercise all appropriate emergency authorities, as well as other relevant authorities, to reduce the number of deaths and minimize the devastation the drug demand and opioid crisis inflicts upon American communities." The opioid

crisis continues to present immense patient harm and fiscal cost to the FEHBP. The OIG Office of Investigations prioritizes cases related to the opioid epidemic to protect the FEHBP and Federal employees, retirees, and their dependents harmed by the crisis, including from the ancillary FWA schemes that emerged in the epidemic's wake.

From 2012 through 2018, approximately:

- \$151.2 million was spent on opioid antagonist prescriptions (e.g., naloxone);
- 26,000 FEHBP enrollees received emergency department care for an opioid overdose; and
- \$11 million in emergency department hospital costs were attributable to FEHBP enrollees who experienced an opioid overdose.

OPM's recent efforts to address the opioid crisis include:

- Utilization review newsletters on a variety of treatment topics, including drug disposal;
- New Health Effectiveness Data and Information Set (HEDIS) measure of opioids added to the Plan Performance Assessment Farm Team; and
- Guidelines for the OPM Call Letter that set the terms of FEHBP carrier contracts.

While the OIG continues to oversee the efforts and implementation of carrier programs and procedures for the prevention and treatment of opioid addiction, OPM and the FEHBP carriers must continue to consider and use preventive measures such as drug formulary reviews, preapproval of opioid-related prescriptions, increased access to medication-assisted therapy, and less-addictive and alternative pain medications. OPM is unable to determine the actual impact of the opioid epidemic on the FEHBP because the agency lacks a single data repository or system to capture a complete, integrated view of program data. This data is needed to effectively and independently manage the FEHBP and determine the impact of a global crisis (like the opioid epidemic) on the program.

The improvements OPM promotes to combat the opioid crisis rely on carriers and subcontractors' adherence; this relates directly to our concerns regarding OPM oversight of how carriers and related entities prevent, target, and report FWA. The complicated and layered nature of carriers and subcontractors should encourage OPM to explore a

single data repository for claims information and a dedicated program integrity office to provide a single source of internal controls, oversight, and trend analysis as part of agency efforts to combat the opioid crisis.

In the FY 2018 Top Management Challenges, we included that PBMs “may find themselves defending future lawsuits alongside the drug manufacturing industry.” Although the current Administration’s medical liability reform proposal may ultimately assist FEHBP carriers in limiting liability, it would not affect the FEHBP until the beginning of 2022. The expansion of local and State opioid-related lawsuits should encourage OPM, as well as FEHBP carriers and subcontractors, to hasten the implementation of preventive measures.

## II. INTERNAL CHALLENGES

The following challenges relate to current program activities that are critical to OPM's core mission, and while impacted to some extent by outside stakeholders, guidance, or requirements, they are OPM challenges with minimal external influence. They are areas that once fully addressed and functioning will in all likelihood be removed as management challenges. While OPM's management already expended a great deal of resources to meet these challenges, and made some notable improvements, they will need to continue their efforts until full success is achieved. This year, the Procurement Process for Benefit Programs challenge and the Health Claims Data Warehouse challenge have been removed as top management challenges.

This FY there are four changes in the internal top management challenges. First, due to successful efforts by OPM to rebid several of the Federal benefit contracts, the Procurement Process for Benefit Programs challenge has been removed as a top management challenge for this year. Second, because the agency has not been able to collect data for the Health Claims Data Warehouse project, it has been removed as a top management challenge until it becomes operational. Third, the transfer of NBIB to DOD also involves the transfer of OPM's legacy systems and data to NBIB. Because the legacy systems are tightly integrated with other OPM systems, this will be a significant short-term challenge for the agency. Fourth, the problem of unentitled people receiving benefits from the FEHBP must be addressed. This is a high risk for the program and there have been several OPM OIG audit findings and investigations related to this problem within the program. OPM addressing this challenge should result in substantial savings of tax payer dollars.

### 1. INFORMATION SECURITY GOVERNANCE

Information security governance is the overall framework and supporting management structure and processes that are the foundation of a successful information security program. Proper governance requires that agency management is proactively implementing cost-effective controls to protect the critical information systems that support the core mission, while managing the changing risk environment. This includes a variety of activities, challenges, and requirements, but is primarily focused on identifying key roles and responsibilities and managing information security policy development, oversight, and ongoing monitoring activities.

In the FY 2018 Federal Information Security Modernization Act (FISMA) audit report, we noted that 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, we also observed that OPM has struggled to implement an IT security governance program to ensure that these controls remain effective, and reported a material weakness in this area.



In FY 2019, OPM's Office of the Chief Information Officer (OCIO) made some progress to improve its IT security governance program, including completing a gap analysis to identify additional resources needed and developing a mechanism to secure the needed funding. The OCIO also demonstrated that there was at least a valid authority to operate for every major system in its system inventory and made limited progress implementing corrective action for previously identified weaknesses. However, more work is needed, especially in the area of information security continuous monitoring, maturing the process of implementing corrective action for identified security control weaknesses, contingency planning, and eliminating the problem of "shadow IT."<sup>3</sup>

We also noted in the FY 2018 FISMA report that these issues result from OPM management's inadequate investment in the agency's IT environment for many years and OCIO's lack of control over the IT budget process. There is no real chargeback methodology, service catalog, or cost accounting process that would clearly and reliably determine the true cost of providing IT services to OPM program offices. As a result, OPM continues to struggle to implement a mature and consistent IT security program.

OPM's CIO has communicated a strategic vision that addresses some of these concerns. OPM's challenge going forward will be to ensure that there are adequate resources available to implement the vision that has been laid out.

## **2. INFORMATION SECURITY CONTINUOUS MONITORING**

In 2011, the National Institute of Standards and Technology introduced the concept of information security continuous monitoring (ISCM) as a strategy to determine the effectiveness of system security controls and to provide information needed to quickly correct inadequate controls. This new approach was intended to replace the triennial system security assessment and authorization (Authorization) process that evaluates whether a system's security controls are meeting the security requirements of that system.

OPM has not fully implemented ISCM, but has developed a strategy that addresses the monitoring of security controls at the organization, business unit, and individual information system level. However, the agency has not successfully implemented several key objectives. During the FY 2019 FISMA audit, the OCIO provided evidence of continuous monitoring activity for only 28 of OPM's 47 major systems. Of those 28, only 8 systems were subject to adequate security controls testing and monitoring in compliance with OPM policies, procedures, and submission schedules.

---

<sup>3</sup> "Shadow IT" is a term that refers to IT applications and infrastructure that are managed and utilized without the knowledge of the enterprise's IT department.

Eight years after the National Institute of Standards and Technology published its ISCM framework, OPM has not implemented a mature ISCM process. Not only that, the agency continues to struggle with the outdated Authorization process. In recent years, OPM's Authorization program has shown some improvement, but overall it continues to be hampered by incomplete and inconsistent results.

During our FY 2019 FISMA audit, we determined that OPM has a current authority to operate for all systems in its major system inventory. While this is a notable achievement, the quality of the authorization packages is questionable.

We acknowledge OPM's efforts and focus on improving its IT security program, including ISCM. The challenge going forward will be for OPM to establish a mature process for properly managing the security of its major computer systems and moving from the outdated Authorization program to fully implementing ISCM.

### **3. DATA SECURITY**

Since the data breaches in 2015, where the personal information of more than 20 million people was compromised, data security has been a top management challenge facing the agency. Significant improvements have been made in the past four years to address the most acute vulnerabilities. OPM has:

- Implemented security tools associated with the Department of Homeland Security's Continuous Diagnostics and Mitigation program to automate security of the agency's network;
- Consolidated nine data centers to seven to comply with the Office of Management and Budget's (OMB's) Data Center Optimization Initiative;
- Encrypted data at rest and in transit supporting the agency's most sensitive systems; and
- Implemented multifactor authentication for network access via Personal Identity Verification (PIV) credentials.

Despite these improvements, OPM's technical environment remains complex and decentralized, characteristics that make it extremely difficult to secure.

The control that would have the greatest impact in securing sensitive data is the full implementation of two-factor authentication. Enforcing the use of PIV authentication to connect to the agency's network is not sufficient, as users or attackers that do gain access to the network can still access OPM applications containing sensitive data with a simple username and password. If PIV authentication were put in place at the application level, an attacker would have extreme difficulty gaining unauthorized access to data without having physical possession of an authorized user's PIV card.

Our FY 2019 FISMA audit showed that application-level multi-factor authentication is in place for fewer than 10 percent of OPM's major computer systems. While multi-factor authentication to the network and the other controls cited by OPM are clear examples of improved perimeter security controls, they are not enough to prevent unauthorized access to sensitive data. Networks are becoming more complex with increased remote access and the adoption of cloud and hybrid infrastructure. Most IT security experts operate under the assumption that their perimeter is or will be compromised, so properly securing applications and data is of equal or greater importance. OPM has noted that it cannot fully implement multi-factor authentication because many of its legacy applications do not support that technology. This situation further demonstrates the importance of OPM's IT Infrastructure Improvement Project discussed below.

#### **4. INFORMATION TECHNOLOGY INFRASTRUCTURE IMPROVEMENT PROJECT**

For the better part of the past decade, OPM acknowledged that its network infrastructure needed a complete overhaul and migration to a much more centralized and manageable architecture. This need was amplified in light of the data breaches of 2015. OPM's initial attempt to modernize its infrastructure involved the creation of two new physical data centers designed to house a modern, centralized, and secure logical network environment to host OPM's systems. However, after more than a year of effort and over \$45 million paid to the sole-source contractor managing the project, OPM recognized that this model was not sustainable and abandoned the entire project before a single application was modernized and migrated.

In the time since, the path to modernization changed with each new Chief Information Officer. With seven individuals in that role since 2015, the lack of continuity has been a significant hurdle. While each CIO has approached modernization through a slightly different lens, largely OPM has focused its efforts on consolidating its existing data centers and dedicating resources to cyber security tools and personnel. This leaves antiquated legacy application modernization at the forefront of the agency's challenge.

In FYs 2017 and 2018, Congress made \$11 million and \$21 million, respectively, available to OPM for IT system modernization, but the obligation of this money was contingent upon the agency developing a comprehensive plan that, among other requirements, identified the full scope and cost of the IT modernization and stabilization project. Our oversight of OPM's IT modernization process has revealed a lack of understanding and adherence to project management and budgeting principles, especially OMB's Capital Planning and Investment Control process.

OPM's current CIO has outlined a reasonable, risk-based IT modernization strategy, including the agency's mainframe environment and the legacy applications that run on it. The strategy also addresses longstanding weaknesses in properly funding the agency's IT operations by implementing the concept of Technology Business Management, which is a framework for establishing the true cost, quality, and value of IT to the supported business operations. We agree that the CIO's vision would conceptually resolve many of the agency challenges we have reported in our FISMA audit report and other related reports; however, the vision must be supported by adequate project planning and funding based on established budget principles.

Even with these positive developments, OPM faces enormous hurdles in reaching its desired outcome of modernizing its legacy infrastructure and applications. The complexity not only involves stabilizing core elements of an effective IT program, but planning and executing the migration of mission critical legacy IT systems to modern technology. Continued turnover in key OCIO positions only exacerbates a difficult situation. As noted in the 'Data Security' challenge discussed above, OPM cannot achieve a mature and effective IT security program without modernizing its antiquated IT systems.

## **5. NATIONAL BACKGROUND INVESTIGATIONS BUREAU LEGACY INFORMATION SYSTEMS**

The transfer of the IT systems that support the NBIB to the DCSA will be a major management challenge for OPM for the near future. It is our understanding that DCSA is in the process of developing a new IT infrastructure and systems to support the background investigations process over the next several years. Until such time that those systems are operational, DCSA will rely on the legacy OPM NBIB systems.

Complicating the transfer is that the NBIB systems reside on OPM's mainframe, which are tightly integrated with other OPM legacy systems. OPM's CIO indicated that the plan is to untangle the NBIB systems from these other systems and transfer responsibility for hosting and managing them to DCSA. While this does make some sense, it will be technically challenging and costly to achieve.

Until that happens, OPM will be responsible for continuing to operate these systems. OPM and DCSA have worked out a chargeback model to provide funding to cover OPM's operating costs. OPM will also be responsible for maintaining and improving logical and physical security over these systems, contingency planning, and environmental controls that support the hardware. This is likely to be a major management challenge in an uncertain situation for an unknown period of time.

## **6. STOPPING THE FLOW OF IMPROPER PAYMENTS**

### **Federal Employees' Retirement System and the Civil Service Retirement System**

In FY 2018, Retirement Services lowered its reported improper payment amount from the Civil Service Retirement and Disability Fund (the Retirement Trust Fund) from \$313.8 million (FY 2017) to \$284 million. The improper payment rate had a corresponding decrease from 0.38 percent (FY 2017) to 0.36 percent (FY 2018). While this improper payment rate is low compared to other Federal benefit-paying agencies, it still places the retirement program in a high-risk category for improper payments.

Even though Retirement Services notes its relatively low improper payment rate, a previous Improper Payments Elimination and Recovery Act audit recommended increased controls to identify the root causes of improper payments and to ensure that the improper payment amount is properly categorized in OPM's Agency Financial Report. However, Retirement Services asserts that its ability to categorize additional root causes is limited because of the existing legacy systems. Without accurate recognition of the root causes of improper payments, it is probable that the improper payment rate is improperly calculated and understated. In addition, identification of the root causes will help OPM develop and implement strategies to prevent future improper payments.

There is an on-going need for innovation and improvement in the analysis of annuity payments. The addition of the Fraud Branch to the Retirement Services program office highlights the agency's attempts to improve its program integrity. Continued progress in this area will help reduce improper payments and tighten control over program vulnerabilities. However, a significant number of OIG investigative cases involve improper annuity payments made over long periods—in some cases, years or even over a decade. The OIG's success in developing proactive investigations and referring the cases to Retirement Services for recoveries demonstrates that improved prevention and detection controls within the program office will lead to the discovery and recovery of, and prevention of future, improper payments.

Retirement Services' resources focused on the pending adjudication of retirement cases, in order to resolve its ongoing backlog of unprocessed retirement applications, are significant.

However, more staff and/or better tools that perform program integrity functions may reduce improper payments substantially.

We recognize core problems that cause improper payments in the retirement programs. The lack of a comprehensive, centralized tracking system to record and analyze program integrity (including appropriate internal control procedures for the timely detection, identification, and reporting of potential FWA) is still an issue.

### **The Federal Employees Health Benefits Program**

The OIG remains concerned that the improper payment rate stated by the agency is inadequate and not reflective of the true amount of improper payments. OPM calculated its total FEHBP improper payments at \$71.44 million in FY 2018 (a 0.14-percent improper payment rate), a substantial increase from FY 2017 (\$28 million in improper payments; a 0.05-percent improper payment rate). The milestones Healthcare and Insurance is seeking in working with OMB to change calculations of the improper payment rate are positive steps.

However, we continue to emphasize the need for a global program integrity office that oversees the FEHBP. A program integrity office (such as one modeled on the Centers for Medicare and Medicaid Services' Center for Program Integrity) will help in identifying improper payments in order to develop a more accurate improper payment rate. OPM has acknowledged our suggestion of an independent program integrity unit has merit, but states that funding and other constraints preclude its creation at this time. We recommend the agency seek out additional funding and take actions to overcome the unspecified additional constraints, engaging all necessary internal and external stakeholders in the process.

In addition to the creation of a program integrity office, there are also legislative remedies that may improve independent oversight of FEHBP contractors and subcontractors. In the past, we recommended that OPM should pursue inclusion of the FEHBP into the definition of a Federal program under the Social Security Act section 1128B(f). We continue to suggest this remedy or others as Healthcare and Insurance deems necessary.

## **7. RETIREMENT CLAIMS PROCESSING**

OPM's Retirement Services office is responsible for determining Federal employees' eligibility for retirement benefits; processing retirement applications for Federal employees, survivors, and family members; issuing annuity payments to eligible retirees and surviving spouses; collecting premiums for health and life insurance; and providing customer service to annuitants.

In FY 2018, OPM paid \$77.93 billion in defined benefits to retirees, survivors, representative payees, and families. The timely issuance of annuitants' payments remains a challenge for OPM, especially coordinating retirement benefits between OPM and other agencies for disability benefits and workers compensation. OPM's Strategic Plan (FY 2018 - 2022), Goal 4 objective is to "[i]mprove retirement services by reducing the average time to answer calls to 5 minutes or less and achieve an average case processing time of 60 days or less." OPM appears to remain focused on its internal process improvements and external outreach towards other Federal agencies to meet their goal. While Retirement Services' average case processing time from October 2018 through July 2019 of 56 days meets part of OPM's Strategic Plan Goal 4, the average call answering time of 12 minutes is above the 5 minutes or less identified in Goal 4.

Retirement Services appears to have taken several steps in FY 2019 to strengthen its operations, including:

- Updating the Services-On-Line website user satisfaction survey with additional questions to align with OMB customer experience guidance;
- Implementing a new e-mail system for its call center to assist Services On-Line inquiries and reduce the number of phone calls to the Retirement Information Office; and
- Progressing on its Online Retirement Application, by presenting Agile Sprint 1 of 7 (a time-boxed iteration of a continuous development cycle), with the goal to develop a prototype.

In continuing its efforts, Retirement Services plans to:

- Continue to integrate improvements for correspondence and claims processing;
- Work with the OCIO to investigate technological capabilities to help improve processing time and reduce wait times;
- Continue to provide Federal retirement policy technical assistance to OPM and Congress;
- Perform on-going audits of agency submissions; and
- Provide monthly feedback to agencies and payroll offices and alert them of trends and improvement opportunities.

OPM should continue to work to obtain the necessary resources and technology to ensure that the needs of its customers and stakeholders are met.

## **8. PROCUREMENT PROCESS OVERSIGHT**

The Office of Procurement Operations (OPO) provides centralized contract management that supports the operations and Government-wide missions of OPM, as well as managing OPM's Government-wide Purchase Card program. During FY 2019, OPO has been committed to improving its internal controls and strengthening the procurement process and stated that its leadership has met weekly with OPM leadership to communicate challenges. Moreover, OPO utilizes the Critical Procurement Priorities Executive Steering Group in support of OPM Strategic Goal 4.1, which seeks improved collaboration, transparency, and communication among OPM leadership and the workforce as a way to improve decision-making, and prevent duplicative efforts or inefficient use of resources.

OPO has continued to work with the Internal Oversight and Compliance office to respond to and close audit recommendations reported in the OIG's final reports, including the *Audit of the U.S. Office of Personnel Management's Office of Procurement Operations' Contract Management Process*, Report No. 4A-CA-00-15-041, and the *Audit of the U.S. Office of Personnel Management's Purchase Card Program*, Report No. 4A-OO-00-16-046. As a result, OPO has increased the number of closed out contract files and participated in the cross-agency data cleanup working group led by Office of the Chief Financial Officer to de-obligate funds and reconcile system data. However, closing out contracts and reconciling system data remains a challenge.

The Procurement Information System for Management (PRISM), a contract writing system used by OPO, resides within the Consolidated Business Information System (CBIS), a financial system owned and maintained by the OCIO. PRISM is antiquated and does not support direct reporting to the Federal Procurement Data System - Next Generation. Reporting in the Federal Procurement Data System - Next Generation is required by the Federal Acquisition Regulation, and reporting in PRISM results in manual processing and reconciliation of contract information and financial information in CBIS, increasing the risk of potential discrepancies and difficulty completing contracting processes, such as contract closeout. However, OPO states that the office has continued to be successful in supporting the OCIO's critical IT requirements, with additional support being recently secured through a new partnership with GSA's Centers of Excellence initiative, and it was recently able to secure contractor support for agency-wide closeout efforts.

OPO experienced a moderate level of attrition during the fiscal year and based on OPM's budget projections, it is unlikely that OPO will be in a position to increase its staff beyond



the current level, which could have a major impact on its efforts to address major challenges moving forward.

## **9. FEDERAL EMPLOYEES HEALTH BENEFITS PROGRAM ENROLLMENT AND ELIGIBILITY**

Unentitled family members or other persons enrolled in an FEHBP plan often go undetected due to the difficulty in identifying these ineligible dependents, an area that has always been a high risk for the program. OPM has not published an estimate of how many ineligible dependents receive benefits from the FEHBP or the total cost to the program, despite it being known as an area of substantial fraud. Healthcare and Insurance uses industry-standard estimates regarding ineligible dependents to inform some decision-making regarding ineligible dependents, as seen in Carrier Letter 2014-11 and Federal Register 3059, but the actual percentage of FEHBP dependents who are ineligible is unknown.

Over the past 5 years, the OIG has identified several audit findings related to ineligible dependents age 26 and older whose eligibility to participate in the FEHBP was unsupported. In addition, investigations of ineligible dependent cases found that enrollees are able to change, update, and add dependents directly with health plans, which accept the changes without verification. Recent audit work shows that enrollees are allowed to self-certify dependent eligibility because there are no requirements in place to verify family relationships (e.g., proof of birth, marriage certificates) by Federal agency benefit officers or FEHBP insurance carriers.

OPM should require Federal agency benefit officers to verify the FEHBP eligibility of dependents at the time of initial enrollment by collecting and maintaining relevant documentation (e.g., proof of birth, marriage certificates, etc.). Furthermore, when enrollees add new dependents to a current FEHBP family plan (no plan enrollment change takes place), OPM should require FEHBP carriers to verify the eligibility of dependents by collecting and maintaining supporting documentation. OPM will need to work with its partners (agencies, payroll offices, carriers) to develop and implement a system to verify and maintain supporting eligibility documentation to reduce the aforementioned issues related to unentitled FEHBP enrollments.



## **Report Fraud, Waste, and Mismanagement**

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

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

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

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