



---

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

---

# **Top Management Challenges: Fiscal Year 2018**

**The U.S. Office of Personnel Management's Top  
Management Challenges for Fiscal Year 2018**

**November 05, 2018**

# EXECUTIVE SUMMARY

*The U.S. Office of Personnel Management's Top Management  
Challenges for Fiscal Year 2018*

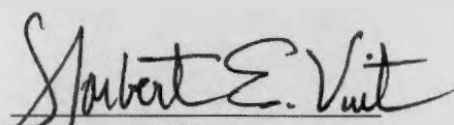
November 05 2018

## **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 three 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; internal challenges, which OPM has more control over and once fully addressed, will likely be removed as a management challenge; and a developing challenge, which is one that has not yet fully materialized.

## **What Did We Consider?**

We identified 12 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**  
*Acting Inspector General*

## **What Did We Find?**

The OIG identified the following three environmental challenges:

- Strategic Human Capital Management;
- Federal Health Insurance Initiatives; and
- Background Investigations.

These environmental challenges are due to such things as rapid technological advances, shifting demographics, various quality of life considerations, and national security threats that are prompting fundamental changes in the way the Federal Government operates. 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 eight internal challenges:

- Information Security Governance;
- Security Assessment and Authorization;
- Data Security;
- Information Technology Infrastructure Improvement Project;
- Stopping the Flow of Improper Payments;
- Retirement Claims Processing;
- Procurement Process for Benefit Programs; and
- Procurement Process Oversight.

Information Security Governance is the only challenge currently reported as a material weakness in the Federal Information Security Management Act (FISMA) report. However, while the remaining challenges are not considered material weaknesses in either FISMA or the CFO Act Financial Statement audit report, they are issues which demand significant attention, effort, and skill from OPM in order to be successfully addressed. Also, there is always the possibility that they could become material weaknesses and have a negative impact on OPM's performance if they are not handled appropriately by OPM management.

Lastly, the OIG identified the proposed OPM reorganization as a developing challenge.

# ABBREVIATIONS

<b>ACA</b>	<b>Affordable Care Act</b>
<b>CHCOC</b>	<b>Chief Human Capital Officers' Council</b>
<b>CISO</b>	<b>Chief Information Security Officer</b>
<b>EPMO</b>	<b>Enterprise Program Management Office</b>
<b>FAST</b>	<b>Federal Action Skills Team</b>
<b>FEDVIP</b>	<b>Federal Employees Dental and Vision Insurance Program</b>
<b>FEHBAR</b>	<b>Federal Employees Health Benefits Acquisition Regulation</b>
<b>FEHBP</b>	<b>Federal Employees Health Benefits Program</b>
<b>FISMA</b>	<b>Federal Information Security Management Act</b>
<b>FLTCIP</b>	<b>Federal Long-Term Care Insurance Program</b>
<b>FSAFEDS</b>	<b>Federal Flexible Spending Account Program</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>HCDW</b>	<b>Health Claims Data Warehouse</b>
<b>HHS</b>	<b>U. S. Department of Health and Human Services</b>
<b>HI</b>	<b>Healthcare and Insurance</b>
<b>HR</b>	<b>Human Resources</b>
<b>ISSO</b>	<b>Information System Security Officer</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>NDAA</b>	<b>National Defense Authorization Act</b>
<b>OCFO</b>	<b>Office of the Chief Financial Officer</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>PIV</b>	<b>Personal Identity Verification</b>
<b>PRISM</b>	<b>Procurement Information System for Management</b>
<b>PBM</b>	<b>Pharmacy Benefit Manager</b>
<b>SSSG</b>	<b>Similarly Sized Subscriber Group</b>

# TABLE OF CONTENTS

	<u>Page</u>
<b>EXECUTIVE SUMMARY</b> .....	i
<b>ABBREVIATIONS</b> .....	ii
<b>I. ENVIRONMENTAL CHALLENGES</b> .....	1
1. STRATEGIC HUMAN CAPITAL MANAGEMENT .....	1
2. FEDERAL HEALTH INSURANCE INITIATIVES .....	2
3. BACKGROUND INVESTIGATIONS .....	8
<b>II. INTERNAL CHALLENGES</b> .....	11
1. INFORMATION SECURITY GOVERNANCE .....	11
2. SECURITY ASSESSMENT AND AUTHORIZATION .....	12
3. DATA SECURITY .....	13
4. INFORMATION TECHNOLOGY INFRASTRUCTURE IMPROVEMENT PROJECT .....	14
5. PROGRAM-WIDE CLAIMS ANALYSIS/HEALTH CLAIMS DATA WAREHOUSE .....	16
6. STOPPING THE FLOW OF IMPROPER PAYMENTS .....	16
7. RETIREMENT CLAIMS PROCESSING .....	19
8. PROCUREMENT PROCESS FOR BENEFIT PROGRAMS .....	20
9. PROCUREMENT PROCESS OVERSIGHT .....	21
<b>III. DEVELOPING CHALLENGE</b> .....	23
OPM REORGANIZATION .....	23

# I. ENVIRONMENTAL CHALLENGES

The following challenges are issues that will in all likelihood permanently be on our list of top challenges for the U.S. Office of Personnel Management (OPM or “the agency”) because of their dynamic, ever-evolving nature, and because they are mission-critical programs.

## 1. STRATEGIC HUMAN CAPITAL MANAGEMENT

Strategic human capital management remains on the U.S. Government Accountability Office’s (GAO) high-risk list of Government-wide challenges requiring focused attention. In order to mitigate the challenge, GAO suggests that OPM, the Chief Human Capital Officers’ Council (CHCOC), and agencies continue taking actions to address skills gaps with respect to capacity, action plan, monitoring, and demonstrated progress.

### **Skills Gaps Closure Strategies Using Data Analysis**

In 2011, OPM partnered with the CHCOC to implement a data-driven strategy for institutionalizing the process for closing skills gaps. In consultation with the CHCOC, OPM launched the multi-factor model assessment tool to assist agencies in identifying their high risk mission critical occupations through the evaluation of a number of different data points. The outcome of the assessment resulted in each agency identifying two to three unique occupations, as well as five Government-wide occupations/functional areas, for skills gaps closure. Each agency formed a Federal Action Skills Team (FAST) to develop and implement a strategy for closing skills gaps in their high risk mission critical occupations, and Occupational Leaders were named for the Government-wide areas.

OPM asserted that they are continuing to monitor and measure the FAST’s progress by agency, as well as on Government-wide skills gaps action plans for Human Resources (HR), Acquisition, Auditor, Economist, and Cybersecurity occupations. This focus includes monitoring evidence-based progress on a quarterly basis with the designated Occupational Leads and Technical Experts, sharing successful practices, and providing tailored technical assistance as needed.

Furthermore, in fiscal year (FY) 2018, to address the HR Specialist skills gaps, OPM produced and marketed 18 staffing courses; developed and launched a new Delegated Examining training and certification; designed a Government-wide HR Policy Center of Excellence pilot; and issued standardized position descriptions and job opportunity announcement templates for the staffing and classification technical areas.

## 2. 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. This year, the Affordable Care Act (ACA) has been removed as a top management challenge. Since the ACA's inception, the number of participating Issuers has steadily declined, and there is only one remaining in the Program as of this year. In addition, the passing enactment of the Tax Bill repealed the individual mandate (starting in 2019), which required most Americans to carry a minimum level of health coverage. Under the ACA, OPM was responsible for implementing and overseeing Multi-State Plan Program options, which began in 2014. The repeal of this mandate will have a significant impact on the individual insurance markets, of which the Multi-State Plan Program is a part. Lastly, there is movement in Congress to defund the Program entirely.

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. While the ever-increasing cost of health care is a national challenge, cost increases in the FEHBP have been relatively modest in recent years. In 2018, OPM announced that the average premium increase for Federal employees and retirees participating in the FEHBP in 2019 would be 1.3 percent, which is the lowest increase since 1996.

It is an ongoing challenge for OPM to keep these premium rate increases in check. 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, the global 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 will require that OPM update guidance and improve its financial reporting activities.



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

Prescription drugs have become a major share of health care costs in the FEHBP, currently representing over 26 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.

Our concern remains that OPM may not be obtaining the most cost effective pharmacy arrangements under the FEHBP. We believe that OPM should consider other options, such as direct contracting with a Pharmacy Benefits Manager (PBM), to gain additional savings and maximize cost containment efforts. Since the inception of the FEHBP, pharmacy benefits have been provided via participating FEHBP carriers by administering pharmacy benefits internally, or by carriers' contracting with PBMs on behalf of their enrolled population. Instead of capitalizing on the purchasing power of over 8 million FEHBP members to negotiate a single PBM contract with OPM, each of the hundreds of FEHBP participating carriers separately contracts with a PBM, with more limited negotiating leverage, resulting in FEHBP pharmacy costs that vary greatly among plans. 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.

Nonetheless, the need for clear and extensive analysis of the FEHBP drug program cost-saving options is long overdue. The last time OPM studied the issue was approximately eight 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, 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.

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

OPM delegates the FEHBP's anti-fraud and program integrity function to all contracted carriers. As such, the program must include strategies to detect and eliminate fraud,

waste, and abuse (FWA) internally by carrier employees and subcontractors, by providers providing goods or services to FEHBP members, and by individual FEHBP members. Carriers must report potential FWA within 30 days to OPM's Office of the Inspector General (OIG). Without a robust FWA program, the FEHBP is at greater risk for increased costs, improper payments, and patient harm to FEHBP members.

OPM recognized the importance of FEHBP carriers having robust FWA programs, and established an internal HI fraud, waste and abuse team to analyze the annual FWA reports from the FEHBP health plans. On November 20, 2017, OPM's HI issued new FWA guidance in Carrier Letter 2017-13. This carrier letter was a collaborative effort between OPM and the OIG to update definitions, reporting requirements, and revamp the annual FWA reporting requirements.

The OIG noted the following FEHBP trends in 2017 related to FWA:

- The number of carrier FWA notifications received by the OIG dropped nearly 74 percent (887 in 2017 versus 3,398 in 2016);
- There was no significant increase in the *quality* of Carrier FWA notifications to the OIG;
- OPM did not require Carrier's to report pharmacy-related FWA "actual savings" in the 2017 Annual Report, one of two primary data points in calculating anti-fraud program Return on Investment; and
- Pharmacy costs rose to 26.2 percent of all FEHBP benefit payments.

In 2017, the President declared a national emergency concerning the opioid epidemic affecting communities across the United States. With the above trends, it must remain a top priority for OPM to hold the FEHBP carriers accountable to provide effective oversight of their PBMs, and PBMs must have a comprehensive fraud detection and prevention program and strategies, track savings, and timely reporting of all potential FWA, especially in relation to the opioid epidemic to the OIG.

FEHBP carriers have more incentive to process and pay claims than to deploy an aggressive program-wide strategy to detect and prevent FWA. In our FY 2017 Top Management Challenges report, we suggested that OPM consider establishing a dedicated Program Integrity Office. Both Medicare and TRICARE<sup>1</sup> have independent and dedicated program integrity units/offices, which deploy comprehensive, self-directed program integrity strategies that enhance oversight initiatives, FWA detection, prevention, and trend analysis. These integrity offices work closely with their OIG's Office of Investigations to enhance oversight and enforcement operations.

---

<sup>1</sup> TRICARE is the civilian care component of the Military Health System.



OPM is fully reliant on the various contracted FEHBP carriers to implement highly inconsistent FWA strategies in a multi-layered environment of subcontractors. This presents a myriad of challenges for OPM to provide meaningful oversight of carriers' FWA programs with no dedicated unit to enforce the necessary guidelines. As such, we think it is important for OPM to consider the benefits of having a dedicated program integrity office to provide independent FWA oversight, ensure consistency with carriers' FWA programs, and track trends and provide accurate data reporting.

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

On June 29, 2011, OPM issued an interim final rule, replacing the Similarly Sized Subscriber Group (SSSG) methodology with what was expected to be a modern and transparent calculation that would ensure the FEHBP received a fair rate. This ruling held 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. Once this rule became effective, audits of the MLR calculation were the only way to determine whether the FEHBP's community-rated carriers were charging fair and reasonable rates to the Program.

However, audits of this calculation for multiple health carriers continue to identify concerns that question how transparent this calculation truly is and whether or not it is a valid method to ensure whether Program participants, as well as the American taxpayers, who are paying approximately 75 percent of the Federal health care premium, are paying a reasonable and fair rate. Specifically, our audits have identified the following:

- Concerns with the accuracy of OPM's subscription income amount used by many carriers in their MLR calculations and whether it includes/should include OPM adjustments to the rates;
- Concerns with the carriers' ability to manipulate the MLR ratio (i.e., through what is reported as capitated costs, claims cost, or FEHBP-specific Federal income tax, 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 Health and Human Services (HHS) guidance that is being used.

We understand and agree that overly prescriptive instructions may not be ideal due to the wide variety of FEHBP carriers operating in a changing landscape and, therefore, some flexibility in deriving MLR percentages should be granted to the carriers. However, the methodologies used not only have to produce accurate results, they should also be auditable. 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.

As stated in last year's Top Management Challenges report, OPM added language to the 2018 rate instructions in an attempt to address our concerns regarding Federal income tax allocation methods. While this is a good first step, the language does not completely resolve all of our concerns with this allocation method and the tax amount that is ultimately used to calculate the MLR. Consequently, carriers using this allocation method to derive their Federal tax expense are likely reporting ratios to OPM that are significantly overstated.

In its response to last year's report, OPM also stated that community-rated carriers' rate build-ups are still subject to audit. However, since an audit of the rate build-up no longer incorporates a comparison of a carrier's FEHBP rates to that of its SSSGs, any audit performed would be nothing more than a math check of the rates, and the results could not be used to determine whether that carrier's subscribers were paying a fair and reasonable cost.

Barring action from OPM to address the above concerns, we will continue to be unable to adequately determine whether MLR is an effective means of ensuring that Program participants are paying a fair and reasonable rate. Therefore, we encourage OPM to assess whether remedies can be implemented to address our concerns, which will result in MLRs that can be used as a basis to measure the fairness and reasonableness of the FEHBP premiums. If this assessment concludes that MLR is ultimately not a viable method to ensure the fairness of the rates, then OPM will need to develop a more appropriate method, as well as sufficient guidance and criteria to regulate its use.

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

Addressing the opioid abuse epidemic has become a top priority for the OIG's Office of Investigations. In the October 2017 President's Memorandum, *Combating the National Drug and Opioid Crisis*, the President described the opioid crisis as a public health emergency and directed a multi-agency response to combat the drug demand and opioid problem afflicting our nation. The memorandum specifies, "Additionally, the heads of executive departments and agencies, as appropriate and consistent with law, 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.”

In August 2017, the U.S. Attorney General announced the formation of the Opioid Fraud and Abuse Detection Unit. The unit focuses solely on health care fraud related to prescription opioids, including pill mills, illegal importation of Fentanyl, and unlawfully diverted or dispensed prescription opioids for illegitimate purposes.

The opioid epidemic has had a large impact on the FEHBP, on both program costs and patient harm. For example, the illegal importation of drugs like Fentanyl from China is not just sold on the streets, but it is also sold to pharmacies, providers, and pain clinics, at reduced costs to dispense to unsuspecting patients. These drugs pose a very high danger of patient harm.

On January 23, 2018, OPM issued an All Carrier Call Letter that emphasized the opioid epidemic and its impact on the FEHBP. The call letter included efforts the carriers must take to prevent opioid misuse and treat addiction. In February 2018 FEHBP carriers briefed OPM and the OIG on the impact of the opioid crisis on the FEHBP. Some important facts presented were:

- The largest FEHBP carrier reported a 300 percent increase from 2012 through 2017 in the identification of beneficiaries potentially abusing prescription opioid medications;
- The number of prescriptions for Narcan, Nalaxone and Evzio, drugs used to thwart opioid-related overdoses, doubled from 2016 through 2017; and
- In 2017, the percentage of FEHBP members enrolled in employee organization fee-for-service plans taking opioid prescriptions ranged between 17.8 percent and 24.3 percent of total beneficiaries.

These statistical indicators are a cause for concern as the OIG has seen little in the way of fraud or patient harm related case notifications from our contracted carriers. The same carriers provide primary oversight of the PBMs administering pharmacy benefits on behalf of over 8.2 million Federal employees, retirees and their eligible dependents. This may be an indicator of a lack of proactive measures being deployed by FEHBP carriers to detect fraudulent providers who may be running pill mills or pharmacies purchasing and dispensing high volumes of opioid medications.

Additionally, ancillary costs for treatment of substance abuse have risen sharply at a rate of nearly 283 percent, from 2013 through 2016, according to the briefing provided by the Blue Cross Blue Shield Association in February 2018. This coincides with a sharp rise in fraud related to opioid addiction treatment with Sober Homes, Outpatient Substance

Abuse Treatment, and Urinary Drug Testing Laboratories inflicting high impact financial losses on the FEHBP. In Florida alone, the OIG received at least 65 fraud allegations related to Sober Home and Substance Abuse Treatment facilities since 2016, providing unnecessary drug tests and other services totaling over \$34.9 million in potential fraudulent FEHBP benefit payments.

Another recent concern is a trend placing responsibility for the opioid epidemic on the health insurance industry. Pharmacy benefits and formularies that restrict or do not reimburse for higher cost, less addictive pain medications, but alternatively offer low cost, highly addictive opioid pain medications, without restrictions, may find themselves defending future lawsuits alongside the drug manufacturing industry. These trends may ultimately have the effect of increasing overall program costs, placing an emphasis on detecting and mitigating fraud, and other strategies to lower costs.

In FY 2019 and 2020, the OIG will continue to oversee the efforts and implementation of new programs and procedures by carriers for fraud detection, prevention, and treatment of opioid addiction. However, OPM and FEHBP carriers must also consider preventive measures that include drug formulary reviews, pre-approval of opioid-related prescriptions, and access to less addictive alternative pain medications for FEHBP members.

Finally, OPM is responsible for providing primary oversight of the FEHBP carrier contracts. However, FEHBP carriers are directly responsible for providing oversight of their contracted PBM. Oversight of these complex, multi-layered, sub-contractual relationships can create barriers and challenges; therefore, a dedicated program integrity office could provide a single source of internal controls, oversight and trend analysis to help OPM mitigate the effects of the opioid crisis on the FEHBP.

### **3. BACKGROUND INVESTIGATIONS**

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

In January 2016, after an interagency review conducted in response to the 2015 OPM data breaches, the Obama Administration announced the establishment of the National Background Investigations Bureau (NBIB) within OPM. NBIB would serve as the new Government-wide service provider of background investigations. With its roles and responsibilities subsequently established formally by Executive Order 13741, NBIB began operating on October 1, 2016, assuming the functions, personnel, and assets of its predecessor the Federal Investigative Services.

Since its establishment, NBIB has taken several steps to make the background investigation process more efficient and to better secure sensitive data in its possession. These steps include the application of a new organizational structure to bolster security and intergovernmental communications. Additionally, since its inception, NBIB has worked closely with the U.S. Department of Defense (DOD) on the development of a new end-to-end IT system, the National Background Investigations System, to support investigative operations and enhance processes.

These developments notwithstanding, the National Defense Authorization Act (NDAA) for FY 2017 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, the NDAA for FY 2018 directed DOD, in consultation with OPM, to begin carrying out the implementation plan no later than October 1, 2020, and granted DOD authorization to conduct background investigations for DOD-affiliated personnel.

On June 21, 2018, the Executive Office of the President published *Delivering Government Solutions in the 21<sup>st</sup> Century: Reform Plan and Reorganization Recommendations*, which proposed to transfer the remainder of NBIB's background investigation functions from OPM to DOD. In doing so, the Administration seeks to retain economies of scale, better leverage existing DOD capabilities, and facilitate the implementation of reforms.

Assuming the handover of the background investigations function proceeds according to the Administration's plan, OPM will face the challenge of efficiently transferring NBIB caseload and assets to DOD, while coping with the impact that transfer will have on OPM's resources. The OIG will work with our counterparts at the DOD OIG and monitor the planned transfer closely to ensure the process is undertaken effectively and consistent with relevant law.

## **B. Case Processing Backlog**

In addition to the efforts mentioned above, NBIB executed a multi-pronged approach to addressing the case management backlog of over 700,000 cases at times during 2017. NBIB's response to Section 3 of the *Securely Expediting Clearances Through Reporting Transparency Act of 2018*, or the "SECRET Act of 2018" (Public Law 115-173), addressed numerous factors that impacted the amount of time needed to carry out investigations, including but not limited to the size of the investigative workforce, the increased complexity of case types, and the IT systems that support background investigations. During our "Audit of NBIB Backlog of Background Investigation Cases

and the Effectiveness of the Quality Assurance Process,” we found these factors to be valid challenges in regards to NBIB’s processing of background cases.

NBIB’s inventory is a result, in part, of not having the investigator capacity on hand in the past to meet the workload demands for investigations and the discontinued use of the contractor services of the US Investigations Services, which was responsible for about 65 percent of the contractor workload. NBIB stated that they addressed this by increasing the capacity of its investigative workforce from 5,843 Federal and contractor investigators on October 1, 2016, to over 8,400 today.

Conducting background investigations relies heavily on both internal and external processes that can delay completion of the investigation. These challenges include but are not limited to: the availability of current OPM legacy IT systems and the delivery of the National Background Investigations System; lack of automation for external record providers such as state and local criminal records; receiving incomplete or inaccurate information via security forms from the applicants; the availability of applicants and sources due to overseas deployments and change of duty stations; and locating key sources for interviews to corroborate issues in complex cases. Additionally, the implementation of the 2012 Federal Investigative Standards, which uses a tiered model and issue flagging strategy, added an increased level of complexity to case work as additional investigative elements were required to meet standards. These are just a few NBIB management challenges that have affected achieving a healthy working inventory.

NBIB should continue to work to improve the timeliness of investigations by optimizing its total workforce capacity, coordinating with stakeholders to create efficiencies within its current end-to-end investigative process, and participating in agency-wide efforts to revamp the entire Federal vetting enterprise.



## 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.

### 1. INFORMATION SECURITY GOVERNANCE

OPM relies on information technology to manage its core business operations and deliver products and services to many stakeholders. With continually increasing reliance on information systems, growing complexity, and constantly evolving risks and threats, information security continues to be a mission-critical function. Managing an information security program to reduce risk to agency operations is an ongoing internal management challenge.

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 proactively implements 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.

For many years, we reported increasing concerns about the state of OPM's information security governance. Our Federal Information Security Management Act (FISMA) audit reports from FY 2007 through FY 2013 reported this issue as a material weakness. Some improvement was demonstrated in FY 2014 and information security governance was upgraded to a significant deficiency in the Agency's overall security posture. OPM has since centralized its cybersecurity program under a Chief Information Security Officer (CISO) that is supported by a team of Information System Security Officers (ISSOs) and network security engineers. This team developed policies and procedures designed to improve the efficiency with which this team operates, and implemented technical security tools and controls that help protect the agency from cyber-attack.

However, based on our FY 2018 FISMA audit, we determined that OPM's information security governance program regressed, and once again, we consider it to be a material weakness in the design and operation of the agency's internal controls. There is no

permanent CISO, and there is an inadequate separation of duties because the current acting CISO is also in charge of IT infrastructure. In addition, OPM continues to struggle in implementing long-standing cybersecurity controls required by FISMA, relapsed in risk management, and received low maturity level scores for continuous monitoring and contingency planning. Furthermore, OPM is not making substantial progress in implementing our FISMA recommendations from prior audits. There are outstanding audit recommendations that are over a decade old, and OPM has not implemented corrective action on a single recommendation from the FY 2017 FISMA audit.

According to OPM, “The OPM [Chief Information Officer] CIO fully understands the importance of information security governance and is taking steps to continue to enhance the governance posture. As part of the FY 2017 and FY 2018 IT Modernization Plans, the CIO has awarded a task to a professional services firm to assist the [Office of the Chief Information Officer] OCIO with establishing an overall IT governance process, a risk management practice, IT enterprise architecture and establishment of an Enterprise Program Management Office (EPMO). As part of the risk management practice, the contractor is assisting the CIO with developing a strategy to close the outstanding findings and [Plan of Action and Milestones] POAMs, as well as a process to ensure the continual focus on the findings and POAMs. In addition, this issue is one of the CIO's top five priorities. Examples of accomplishments have been the implementation of a multi-tiered change management process that focused on reviewing all changes to the technical environments; implementation of additional cybersecurity policies and procedures; approval of hiring for vacant ISSO positions; and implementation of a multi-tiered process for reviewing all potential closures of POAMs.”

We acknowledge the effort and focus that the OCIO is placing on improving its overall IT governance program. While it is possible that this will result in a sustained improvement leading to a fully mature IT security program, given OPM's inconsistent history and high turnover in key positions, it will be a major challenge going forward.

## **2. SECURITY ASSESSMENT AND AUTHORIZATION**

Information system security assessment and authorization (Authorization) is a comprehensive assessment that evaluates whether a system's security controls are meeting the security requirements of that system. In recent years, OPM's Authorization program has shown some improvement, but overall it continues to be hampered by incomplete and inconsistent results.

In FY 2016, OPM initiated an “Authorization Sprint” designed to bring all of the agency's systems into compliance with Authorization requirements. OPM dedicated significant

resources toward re-authorizing the systems that were neglected. By the second quarter of FY 2017, the OCIO completed an Authorization for every major information system owned by the agency, and successfully addressed some of the critical weaknesses that our audits identified with the previously completed Authorization packages.

As a result of these improvements, in FY 2017 we removed a material weakness related to system Authorizations that had been reported in several prior FISMA audit reports. We still considered the issue a significant deficiency in both FY2017 and FY 2018 however, primarily because of incomplete or inadequate independent testing of the systems' security controls.

According to OPM, "The OPM CIO continues to work to improve the [Authorization to Operate] ATO program. In addition to the previous improvements to the ATO process, the CIO has placed emphasis on completing the contingency testing portion of the ATO process and on fully documenting penetration testing. As part of the FY [20]17 and FY [20]18 IT Modernization plan, the CIO has awarded a contract to improve IT governance. The support under this task includes establishing a risk management practice and assistance with addressing all of the open findings and POAMs from all sources (OIG, GAO, annual financial audits, etc.). Addressing all open findings and POAMs is one of the CIO's top five priorities and the entire OCIO organization is working diligently to address the issues. The ATO findings are included in these efforts."

We acknowledge that OPM started the process of improving its IT governance, which should result in more consistent results in several areas, including its Authorization program. However, given the many years of inadequate performance and halting progress it remains to be seen whether OPM will be able to establish a mature process for properly managing the security of its major computer systems.

### **3. DATA SECURITY**

In 2015, OPM was the victim of devastating data breaches in which the personal information of more than 20 million people was compromised. OPM's technical environment is complex and decentralized, characteristics that make it extremely difficult to secure. OPM subsequently implemented security tools associated with the Department of Homeland Security's Continuous Diagnostics and Mitigation program to automate security of the agency's network.

While OPM made some progress encrypting the databases that support the agency's most sensitive systems, controls to encrypt data at rest and in transit have not been implemented.

Even when full encryption is in place, though, it would not completely protect sensitive data, since the compromise of a valid user's password could allow an attacker to decrypt the data.

The control that would have the greatest impact in securing sensitive data is the full implementation of two-factor authentication via Personal Identity Verification (PIV) credentials. OPM enforced the use of PIV authentication to connect to the agency's network. However, this control in itself 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.

OPM states that it "... continues to implement multifactor authentication for access to applications, as well as other security controls. Multifactor authentication for network access is an important security control that when combined with other controls such as network segmentation, separation of privileged accounts, and reduction of privileged accounts, creates a significantly improved cybersecurity posture. The largest challenge with fully implementing multifactor authentication for all of OPM's applications is the ability of legacy applications and technology to support multifactor authentication. OPM continues to identify technologies that will enable legacy applications to utilize multifactor authentication."

Our FY 2018 FISMA audit showed that application-level multi-factor authentication is in place for only 6 of OPM's 54 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 asserts 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 Modernization Plan (see challenge number 4, below).

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

Prior to the 2015 data breach, OPM determined that its network infrastructure ultimately needed a complete overhaul and migration into a much more centralized and manageable architecture. 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 OPM suspended its dual commercial data center approach, the agency has focused its efforts on consolidating its nine existing data centers and dedicating resources to cyber security tools and personnel.

In FY 2017, Congress made \$11 million 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. To document OPM's adherence to these basic project management and capital budgeting activities, Congress included in the FY 2017 Omnibus Appropriations Act the requirement for certain artifacts, including an OMB Major IT Business Investment (OMB Exhibit 300). The FY 2018 Appropriations Act included another \$21 million for modernizing OPM systems subject to similar requirements.

OPM's FY 2017 and FY 2018 IT modernization spending plans did not fully address the Congressional requirements. OPM officials told us that the agency's IT environment was so fractured and decentralized, and so lacking in overall governance, that they were not able to even begin the process of designing an overall IT modernization plan. The capital planning and investment control process that is described in Office of Management and Budget (OMB) Circular A-11, and which forms the basis of the FY 2017 and 2018 Appropriations Act requirements, could not be implemented. We were told that technical analysis, and cost and schedule estimates, were impossible.

We expressed the opinion that Congress should allow the agency to obligate the FY 2017 and FY 2018 funding subject to the proviso that it develop an EP MO with the goal of developing IT governance policy and defining an overall IT enterprise architecture. We can confirm that in FY 2018 OPM awarded a contract to a vendor to begin the process of establishing an EP MO with those objectives.

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,' OPM cannot achieve a mature and effective IT security program without modernizing its antiquated IT systems.

## 5. PROGRAM-WIDE CLAIMS ANALYSIS/HEALTH CLAIMS DATA WAREHOUSE

The challenge for OPM is that while the FEHBP directly bears the cost of health care services, it is in a difficult position to analyze those costs and actively manage the Program to ensure the best value for both Federal employees and taxpayers, because OPM has not routinely collected or analyzed program-wide claims data. The Health Claims Data Warehouse (HCDW) project is an initiative to collect, maintain, and analyze data on an ongoing basis to better understand and control the drivers of health care costs in the FEHBP.

Because the data collected in this system is highly sensitive protected health information, it is critical that it be protected from improper disclosure. According to OPM's Healthcare and Insurance (HI) office, "OPM's [Office of the Chief Information Officer] OCIO has implemented multiple improved layers of security on the technical infrastructure such as intrusion prevention and detection, multifactor authentication through PIV, third generation firewalls, automated security patching and data loss prevention for improved infrastructure management and protection of data contained within the HCDW. In addition to the above improved security measures, HI works closely with OPM's Cybersecurity Program to continue to strengthen and ensure the latest security policies, practices and measures are in place to protect the HCDW."

While this is generally true, OPM's challenge going forward is to further strengthen system security as information technology (IT) security threats are constantly evolving. This will be particularly challenging for OPM, as the HCDW resides in a technical infrastructure that has proven very difficult to manage (see the Information Technology Infrastructure Improvement Project challenge starting on page 14 of this report). In addition, we completed an audit of the security controls of the HCDW in FY 2018 and found several areas for improvement in its implementation of recommended security controls.

## 6. STOPPING THE FLOW OF IMPROPER PAYMENTS

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

In FY 2017, OPM paid over \$82.9 billion to nearly 2.6 million Federal annuitants and survivor annuitants under the Federal Employees Retirement System and the Civil Service Retirement System. Payments are made out of the Civil Service Retirement and Disability Fund (Retirement Trust Fund), into which Federal employees and the Government (i.e., American taxpayers) each contribute.

In its Agency Financial Report, OPM reported that the overall improper payment rate for these retirement programs was .38 percent in FY 2017. This rate is a combination of



overpayments and underpayments and is quite low compared to many other Federal programs. However, even though the improper payment rate is low, it still places the retirement program in a high-risk category for improper payments. The total amount of all types of improper retirement payments reported by the agency was \$313.8 million. Of that amount, \$238.7 million, which represented .29 percent, were overpayments. The amount of payments that resulted in underpayments was \$75.1 million, which represented .09 percent.

OPM's Retirement Services office is aware of the major contributing factors to these improper payments; however, it is unable to provide the level of granularity needed to fulfill OMB A-136 reporting requirements. OPM's systems were not designed or built to perform analysis of vast quantities of data.

OPM stated that it is fully committed to identifying the root causes of improper payments. In FY 2018, Retirement Services actively engaged the OCIO to assist with achieving this commitment, and as one step, performed a limited marital certification survey that discovered, identified, and documented overpayments and a savings due to remarriage of the survivor. Additionally, in FY 2016 and FY 2017, Retirement Services performed a 1099R Project, reviewing 1099Rs, which report the amount of annual payments to annuitants, returned as undeliverable in FY 2015 and FY 2016 through the U.S. Postal Service.

However, we continue to believe that the process for conducting projects and reviews such as those described above, and for reporting and following up on the results, needs to be improved. In addition, the need for continuing innovation in the analysis of available information on annuity payments is never ending. The OIG spends a significant amount of time and resources identifying, assessing, and investigating retirement cases where a single deceased annuitant was improperly paid over five, ten, or even twenty years. It is clear that not all improper payments are being identified in a timely manner.

Furthermore, we continue to conclude that Retirement Services lacks a comprehensive centralized tracking system to record and analyze its program integrity work, and lacks appropriate internal control procedures to timely detect, identify, and report potential fraud, waste, and abuse.

OPM management has a duty to the American people to protect the integrity of the retirement trust fund from fraud and waste from improper payments. As such, Retirement Services should consider addressing these issues by establishing a dedicated program integrity office or unit whose sole objective is the detection and prevention of potential fraud, identifying program vulnerabilities, and finding the root causes of improper payments.

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

Until OPM develops a more adequate and reflective improper payment rate, an effective corrective action plan to reduce and recover FEHBP improper payments is not possible. In FY 2017, OPM paid over \$50 billion in medical and pharmaceutical benefits for over 8.2 million Federal employees, retirees, and their dependents. During the same fiscal year, OPM reported an improper payment rate of .05 percent, representing approximately \$28 million, for FEHBP medical and pharmaceutical benefits.

The calculation of improper payments for the FEHBP includes OIG investigative recoveries, OIG monetary audit findings, and monies returned by contracted health plans through the U.S. Department of the Treasury. However, OPM's calculation fails to include improper payments related to payment errors and fraud losses identified but not recovered from FEHBP contractors.

For example, FEHB Program Carrier Letter 2014-11 reported OPM paid approximately \$23 billion in health benefits annually for family members (dependents) enrolled in the FEHBP. OPM stated that health insurance industry standards indicate that up to 10 percent of family members are ineligible for coverage. If that percentage is determined to be true for the FEHBP, health claims of over \$2 billion could be at risk for being improperly paid. OPM recently proposed new regulations that, when notified, carriers would be allowed to prospectively dis-enroll ineligible dependents. However, not requiring FEHBP contractors to retrospectively apply the ineligibility determination allows the FEHBP contractors to ignore these improper payments.

The OIG has consistently found that FEHBP contractors have difficulty identifying, collecting, and tracking overpayments. The OIG and OPM have a mutual interest in protecting the FEHBP from improper payments. However, a longstanding program vulnerability is OPM's limitation in obtaining and integrating FEHBP data needed to independently detect and address improper payments and fraud. OPM must amend its contracts to obtain access to complete FEHBP data so OPM can effectively and independently oversee the program and meet its strategic goals.

OPM must also continue to pursue legislative remedies, such as inclusion of the FEHBP into the definition of a federal program under section 1128B(f) of the Social Security Act, to strengthen its independent oversight of FEHBP contractors.

## 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 approximately 2.6 million annuitants.

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. In January 2012, Retirement Services released and began implementation of its Strategic Plan with the goal of adjudicating 90 percent of retirement cases within 60 days beginning in July 2013. Retirement Services believes that this "challenge is now outdated" and references the new OPM Strategic Plan (FY 2018 - 2022), Goal 4, in which their new 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. However, while Retirement Services appears to have met its average case processing goal for FY 2018, with an average processing time of 59 days, its claims backlog as of September 2018 was 17,628, more than 4.5 percent higher than at the same time a year ago. In addressing the average call answering time, Retirement Services stated that the average time to answer calls in FY 2017 was 9.7 minutes, but it increased to 12 minutes in FY 2018, more than double the strategic plan goal of 5 minutes or less. Again, no data was provided to support Retirement Services' average time to answer calls.

In order to alleviate the excessive busy signals and long wait times, Retirement Services provided more automated services via Services-On-Line, a redesign which went live on June 10, 2018, featuring a new technology stack with responsive design that is compatible with any hand held device, and provides a more customer friendly experience and efficient processing of transactions.

In continuing its efforts, Retirement Services plans to:

- Continue to integrate improvements for correspondence and claims processing;
- Enhance reporting tools to monitor and address Retirement Services workloads;
- Utilize overtime to assist with timely 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 all OPM offices and Congress;
- Perform on-going audits of agency submissions;
- Provide monthly feedback to agencies and payroll offices and alert them of trends and improvement opportunities; and
- Identify training needs for agencies, develop job aids and on-line training modules, and conduct workshops on the retirement application process.

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

## **8. PROCUREMENT PROCESS FOR BENEFIT PROGRAMS**

On October 14, 2015, the OIG issued a Management Alert memorandum to OPM's former Acting Director outlining our continued concerns related to the delays in OPM's benefit program procurements and the failure to properly manage the bid process for the BENEFEDS benefits portal, the Federal Long Term Care Insurance Program (FLTCIP), and the Federal Flexible Spending Account Program (FSAFEDS).

Over the past year, OPM corrected some of the deficiencies in its benefit program procurement process and strengthened its oversight role in monitoring these procurements, including an update to its delegation of authority. OPM's Office of Procurement Operations (OPO) and Federal Employee Insurance Operations collaboratively prepared a corrective action plan addressing the OIG's recommendations found in the Management Alert memorandum, and implemented several controls to mitigate future lapses in bidding actions. So far, three of the four recommendations identified in our Management Alert memorandum have been satisfactorily implemented by OPM and closed. The last recommendation is currently being addressed by OPM and is expected to be finalized in FY 2019.

We commend OPM's efforts to correct these deficiencies in its benefit program procurement process. OPM's challenge moving forward will be multifaceted and involve a need to deliver a long-term, consistent procurement strategy that ensures proper independent oversight, compliance with all applicable regulations, and the timely re-bidding of contracts so that the best value for the Federal Government is achieved. Strengthening the procurement planning process to minimize potential delays is vital to meeting this challenge. Resource requirements within OPO and Federal Employee Insurance Operations will need to be assessed on a regular basis so that OPM can manage multiple procurement actions simultaneously. Any extensions of contract periods of performance or contract modifications

must be justified, be compliant with applicable laws and regulations, and be documented and approved by OPM's oversight authority. The OIG will continue to monitor the progress of the procurement plan as OPM implements additional controls and prepares for future procurements.

## **9. PROCUREMENT PROCESS OVERSIGHT**

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. Prior data breaches that affected over 20 million current and former Federal employees focused a spotlight on the contracts awarded to mitigate the impact of these recent events on those impacted.

OPO has been committed to improving its internal controls. During FY 2018, OPO continued to strengthen oversight of the procurement process by working with the Internal Oversight and Compliance office to address the OIG's audit report recommendations from the *Audit of the U.S. Office of Personnel Management's Office of Procurement Operations' Contract Management Process*, Report Number 4A-CA-00-15-041, issued July 8, 2016. In addition, OPO implemented new policies, which extend its oversight of contracting documents beyond pre-award activities to post-award activities and periodic reviews of contract files, provide guidance on maintaining contract files, establish a consistent contract file format and checklist, and clarify aspects of the procurement oversight process and the role of acquisition team members.

While OPO made progress in strengthening its oversight functions, the systems used to process acquisitions continue to be a major challenge. The Procurement Information System for Management (PRISM), which is the contract writing system used by OPO, resides within the Consolidated Business Information System, a financial system owned and maintained by the OCFO. 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 Regulations, and reporting in PRISM results in manual processing and reconciliation of contract information and financial information in the Consolidated Business Information System, increasing the risk of potential discrepancies and difficulty completing contract closeout. OPO is working with the OCFO and program offices to address system discrepancies between PRISM and the Consolidated Business Information System.

OPO should continue to move forward to (1) hire staff at all levels, secure contractor support for critical OCIO IT requirements and agency-wide closeout efforts, and communicate challenges to OPM leadership; (2) finalize the agency-wide warrant (delegated procurement

authority) refresh<sup>2</sup>, and review and approve drafted Oversight and Compliance Policy (through the Office of the General Counsel and Labor-Management Relations); (3) continue procurement action reviews with OPM program offices, collaborate efforts with OMB/Office of Federal Procurement Policy on their Acquisition 360 initiative and analyze FY 2017 survey data to identify improvement opportunities and strengthen communication; (4) complete the contract close-out process; and (5) leverage the cross agency working group to increase the contract close-outs.

---

<sup>2</sup> The refresh ensures such authority is current and up to date and that it is being properly administered through the established federal acquisition institute training assistance system.



### III. DEVELOPING CHALLENGE

The following new challenge relates to program activities that are critical to OPM's core mission and will affect OPM as a whole.

#### **PROPOSED OPM REORGANIZATION**

In June 2018 the Executive Office of the President published a Government reform plan, titled *Delivering Government Solutions in the 21st Century: Reform Plan and Reorganization Recommendations*. The document puts forward a sweeping plan that would completely reorganize OPM.

First, the plan proposes to transfer OPM's authority with respect to Federal human resources policy to the Executive Office of the President, centralizing in that office matters of employee compensation, workforce management, and the like. Second, the Administration's plan would transfer the functions of Retirement Services, Healthcare and Insurance, and Human Resources Solutions to the General Services Administration, which would be renamed the "Government Services Agency." Lastly, the reorganization plan calls for the transfer to DOD of the remaining background investigation functions performed by NBIB that were not part of the investigation functions moved to DOD with the enactment of the NDAA for FY 2018.

The transfer of any or all of the OPM functions as contemplated by the Administration's plan carries with it the challenge of ensuring that the transfer of functions is accomplished efficiently and in accordance with relevant law. The OIG intends to closely monitor any OPM actions to effectuate the proposed reorganization.



## **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