



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

Top Management Challenges: Fiscal Year 2017

**The U.S. Office of Personnel Management's Top
Management Challenges for Fiscal Year 2017**

November 01, 2017

EXECUTIVE SUMMARY

The U.S. Office of Personnel Management's Top Management Challenges for Fiscal Year 2017

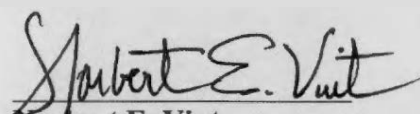
November 01 2017

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 have identified these 11 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 increased globalization, 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.

These internal challenges, while not currently considered material weaknesses, are issues which demand significant attention, effort, and skill from OPM in order to be successfully addressed. 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.

ABBREVIATIONS

| | |
|----------------|--|
| ACA | Patient Protection and Affordable Care Act |
| CHCO | Chief Human Capital Officers |
| CISO | Chief Information Security Officer |
| DOD | U.S. Department of Defense |
| GAO | U.S. Government Accountability Office |
| FEHBAR | Federal Employees Health Benefits Acquisition Regulations |
| FEDVIP | Federal Employees Dental and Vision Insurance Program |
| FEHBP | Federal Employees Health Benefits Program |
| FIS | Federal Investigative Services |
| FISMA | Federal Information Security Management Act |
| FLTCIP | Federal Long-Term Care Insurance Program |
| FSAFEDS | Federal Flexible Spending Account Program |
| FWA | Fraud, Waste, and Abuse |
| FY | Fiscal Year |
| HCDW | Health Claims Data Warehouse |
| HI | Healthcare and Insurance |
| HR | Human Resources |
| ISSO | Information System Security Officer |
| IT | Information Technology |
| MLR | Medical Loss Ratio |
| MSPP | Multi-State Plan Program |
| NBIB | National Background Investigations Bureau |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| OPM | U.S. Office of Personnel Management |
| OPO | Office of Procurement Operations |
| PIV | Personal Identity Verification |
| PPA | Planning and Policy Analysis |

TABLE OF CONTENTS

| | <u>Page</u> |
|--|-------------|
| ABBREVIATIONS | i |
| I. ENVIRONMENTAL CHALLENGES | 1 |
| 1. STRATEGIC HUMAN CAPITAL MANAGEMENT..... | 1 |
| 2. FEDERAL HEALTH INSURANCE INITIATIVES..... | 2 |
| 3. BACKGROUND INVESTIGATIONS..... | 9 |
| II. INTERNAL CHALLENGES | 12 |
| 1. INFORMATION SECURITY GOVERNANCE..... | 12 |
| 2. SECURITY ASSESSMENT AND AUTHORIZATION..... | 13 |
| 3. DATA SECURITY..... | 14 |
| 4. INFORMATION TECHNOLOGY INFRASTRUCTURE IMPROVEMENT PROJECT..... | 15 |
| 5. STOPPING THE FLOW OF IMPROPER PAYMENTS..... | 16 |
| 6. RETIREMENT CLAIMS PROCESSING..... | 17 |
| 7. PROCUREMENT PROCESS FOR BENEFIT PROGRAMS..... | 18 |
| 8. PROCUREMENT PROCESS OVERSIGHT..... | 19 |

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’ (CHCO) Council, and agencies implement specific strategies and evaluate their results to demonstrate progress on addressing critical skills gaps.

Closing Skills Gaps

In April 2017, Title 5, Code of Federal Regulations, Part 250 subpart B was published requiring that program specific workforce investments and strategies (*e.g.*, closing skill gaps) be incorporated into Agency Annual Performance Plans.

The Government-wide and Federal Agency, Federal Action Skill Teams, established in 2016, are currently responsible for providing quarterly updates on their skills gaps closure process, as defined in their action plans to the OPM Director.

OPM has had success in creating an infrastructure and governance structure for closing Human Resource (HR) skills gaps across the Federal government. The agency has built coalitions with professionals across the Federal government to participate in, and collaborate on, activities that will assist agencies in developing strategies over the scope of the five-year strategic plan for closing HR skills gaps. In FY 2016 the framework for the new Delegated Examining Certification Program was approved by the Executive Steering Committee, which consists of leadership from a number of Federal agencies and is staffed by subject matter experts from OPM’s Employee Services’ Strategic Workforce Planning Center, and the CHCO Council. By the end of FY 2016, a proposed Delegated Examining Certification Program of competence was presented to the ESC for closing HR skills gaps. In FY 2017, funding for the new Delegated Examining Certification Program was secured. Also in FY 2017 the closing HR Skills Gaps initiative put greater emphasis on building and maintaining HR Capabilities. HR Capabilities not only looks at skills gaps, but will cultivate continuous development of Federal HR professionals’ capacity to recruit and retain the best and brightest talent to achieve the mission of Federal agencies. In FY 2018 the focus will be on developing the assessment and tracking/registration system for the new Delegated Examining Certification Program, followed by implementation.

According to OPM, through FY 2020, the Federal Action Skills Teams will execute and monitor their action plans, submit quarterly reports to OPM, and review reports with the OPM Director. Because delegated examining is a critical area of non-compliance for staffing specialists, OPM will develop, approve, pilot, and launch a formal Delegated Examining Certification Program and they will continue to post technical competencies and courses to enhance OPM's HR University.

While OPM has made progress in working to close the skills gaps within the Federal Government, OPM should continue to work on branding and communicating the overall effort for equipping the HR community with the tools and resources needed to provide the best service to their customers.

2. FEDERAL HEALTH INSURANCE INITIATIVES

Two major challenges for OPM involve the Federal Employees Health Benefits Program (FEHBP) and the Multi-State Plan Program (MSPP). 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. In addition, with the passage of the Patient Protection and Affordable Care Act (ACA), OPM's roles and responsibilities related to Federal health insurance were expanded significantly. Under the ACA, OPM is responsible for implementing and overseeing MSPP options, which began in 2014. The following sections highlight these challenges and current initiatives in place to address them.

A. 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 2017, OPM announced that the average premium increase for Federal employees and retirees participating in the FEHBP in 2018 will be 4.4 percent, which is down 2 percentage points from the 2017 benefit year increase, which was the largest since 2011.

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 rating methodology will require that OPM update guidance and improve its financial reporting activities.

1) 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.

OPM has made a significant investment in the effort to build an analytical and research data warehouse that will help to fulfill the administrative responsibility of ensuring that FEHBP participants receive quality health care services while controlling the costs of premium increases.

OPM's Planning and Policy Analysis (PPA) group collaborated with OPM's Office of the Chief Information Officer (OCIO) to provide expertise in the areas of system administration, database administration, and networking. PPA and the OCIO completed the development of the HCDW system, and it has been authorized by the Chief Information Officer to run in a production environment. OPM implemented various security features to protect claims data, including data encryption, data masking, and secure authentication mechanisms. The OIG reviewed the security controls of this system and did not detect any weaknesses in the system's ability to protect sensitive data.

OPM's challenge going forward is to further strengthen system security as information technology (IT) security threats are constantly evolving. While this is true for any IT system, it 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 15 of this memo).

OPM will also be challenged with populating the warehouse with big data from a large number of disparate sources, some of which may not be willing to cooperate. Additional challenges involve compliance with Privacy Act requirements and public disclosure related to establishing a new system of records.

2) Prescription Drug Benefits and Costs

Prescription drugs have become a significant portion of healthcare costs, representing over 25 cents of every healthcare dollar spent in the FEHBP. Drug expenditures will likely continue to experience significant increases in the foreseeable future, due in part to new pharmaceutical advancements in biotechnology/biosimilar agents and the rapid expansion of the specialty drug market. OPM will need to develop an effective, long-term strategy to mitigate and manage FEHBP prescription drug costs, while maintaining overall program value and effectiveness.

One opportunity to potentially lower prescription drug costs, to which OPM should give serious consideration, is carving out the pharmacy benefit entirely from the health benefits currently provided by FEHBP carriers.

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 pharmacy benefit managers (PBM) 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.

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. A prescription carve-out program would allow OPM to gain more control of pharmacy benefits by leveraging the purchasing power of the FEHBP in negotiating transparent, flexible, and cost beneficial contract terms and pricing.

We recognize that OPM cannot currently contract directly for prescription drug benefits. However, the vehicle to change that has existed since 2011, when "The President's Plan for Economic Growth and Deficit Reduction" was issued calling for streamlining FEHBP pharmacy benefit contracting and allowing OPM to contract

directly for pharmacy benefit management services on behalf of all FEHBP enrollees and their dependents.

In the past, OPM has sought to amend the current FEHBP law to permit OPM to contract directly with PBMs, but there has not been a concentrated effort by OPM to push this initiative to Congress for approval. We encourage OPM to continue with this effort and work with its Office of Congressional and Legislative Affairs to make the proposed statutory authority language change a priority initiative in 2018.

3) Health Benefits Carriers' Fraud and Abuse Programs

OPM delegates the FEHBP program integrity function to all contracted carriers. As such, the FEHBP insurance carriers must have programs to prevent fraud and abuse, including policy, procedures, training, fraud hotlines, education, and technology. These fraud, waste, and abuse (FWA) programs must follow industry standards and adhere to mandatory information sharing requirements via written case notifications and referrals to OPM's OIG.

Without such programs, there are likely to be increased costs and a greater risk of harm to FEHBP members.

Over the past few years, OPM recognized the importance of FEHBP carriers having effective fraud and abuse programs and partnered with the OIG to develop new, comprehensive fraud and abuse guidance. As a result of this collaborative effort, OPM is in the process of drafting and issuing an updated FWA Carrier Letter (replacing Carrier Letter 2014-29) to all FEHBP carriers. This Carrier Letter will contain updated definitions, training guidance, and reporting requirements.

After reviewing the 2015 and 2016 fraud and abuse reports submitted under the current Carrier Letter 2014-29, it is apparent that the carriers still require additional guidance from OPM. We also found that some carriers are still not reporting fraud and abuse cases appropriately; allow their vendors, such as PBM's, to interpret and report FWA numbers; do not audit or confirm the vendor's reports; and lack oversight of their vendor's FWA detection and reporting efforts. Notwithstanding these issues, there continues to be a significant number of case notifications received from the carriers. This is a direct result of our audit work and the collaboration with OPM. While the quantity of these notifications have remained significant, the carriers still require guidance on submitting *quality* referrals. We are hopeful that OPM's updated FWA Carrier Letter will provide the necessary guidance to assist carriers in

minimizing audit findings, providing quality referrals, and reporting accurate data in FWA annual reports.

OPM has also created a formal Healthcare and Insurance (HI) FWA team that includes representatives from Program Analysis and Systems Support, HI Groups and Audit Resolution, and regularly consults with the OIG. Additionally, OPM/HI reviewed and analyzed annual FWA reports from the FEHB health plans to assess contract compliance and Program performance. One additional action OPM should consider is the establishment of a dedicated Program Integrity Office.

OPM appears to be dedicated to working collaboratively to address this important challenge facing the FEHBP. However, OPM must continue to implement controls that will hold the FEHBP carriers accountable for operating effective fraud and abuse programs. After more comprehensive guidance has been issued, OPM will need to enforce these requirements and hold the carriers accountable. Effective fraud and abuse programs will result in significant cost savings and, more importantly, better protect FEHBP members.

4) Medical Loss Ratio Implementation and Oversight

Each community-rated carrier is held to a specific medical loss ratio (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 or exceed the MLR, it risks returning the excess premiums in the form of a rebate to the FEHBP.

OPM's Office of the Actuaries works closely with OPM's Office of the Chief Financial Officer to confirm that proper accounting for MLR credits and penalties is established to ensure both disbursement and receipts of MLR transactions are appropriately accounted for and documented.

As OPM's MLR methodology matures, and situations unique to the FEHBP MLR continue to surface, the need for detailed criteria and carrier instruction becomes ever more crucial. During recent MLR audits, the OIG identified areas of the MLR methodology that continue to lack clear instruction from OPM, such as tax allocation methods, overage dependent eligibility, and determination of premiums. OPM's rate instructions currently refer community-rated carriers to the Department of Health and Human Services' (HHS) MLR guidelines for issues not covered in the OPM instructions. However, depending upon the issue identified, using the HHS guidance is not always feasible or even applicable.

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 their MLR percentages should be granted to the carriers. However, the methodologies used not only have to produce accurate results, but they should also be auditable. In instances where this is not the case and the resulting issues cannot be adequately addressed by HHS guidelines, then it is incumbent upon OPM to develop its own guidance to address these issues.

Failure to implement clear instructions to address these concerns may result in inaccurate or incomplete subsidization penalties due to OPM or credits that are due to the carriers. Consequently, OPM must stop relying solely on HHS regulations and address these FEHBP-specific problems by providing the necessary guidance via the rate instructions to avoid continued confusion and ambiguity.

To OPM's credit, language was added to the 2018 rate instructions in an attempt to address our concerns regarding Federal income tax allocation methods that were identified on recent audits. While this is a good first step to address this issue, we still have several concerns with OPM's use of MLR as a basis of determining fair and reasonable rates.

Our biggest concern is the fact that in switching from the Similarly-Sized Subscriber Group methodology to an MLR methodology, OPM moved carriers from a community rating method to a more cost accounting-based method. Unfortunately, most of the criteria currently in place for the community-rated health plans provides guidance and instruction for how to develop a community rate, not how MLR confirms that the FEHBP received a fair and equitable community-rate.

There is, however, guidance for experience-rated health plans in the Federal Employees Health Benefits Acquisition Regulations (FEHBAR) which provides direction on allocation techniques and other cost-based accounting methods. Perhaps these sections of the FEHBAR should be amended to also apply to community-rated carriers that are required to file an MLR form with OPM. We believe it should be considered, as the resulting impact would be more concrete guidance on how costs should be allocated, which would result in a more auditable MLR ratio.

OPM must carefully assess the concerns and challenges facing the application of MLR methodology and develop adequate instructions that allow carriers to produce accurate and auditable MLR ratios. If this is not done, the validity of the MLR calculations will continue to be in question, which will more than likely impact the penalties that are truly owed to OPM and the credits that are truly due to the carriers.

B. Affordable Care Act

Under the Affordable Care Act (ACA), OPM is designated as the agency responsible for implementing and overseeing the multi-state plan (MSP) program. In accordance with the ACA, at least two multi-state plans should be offered on each state health insurance exchange beginning in 2014. Multi-state plans will be one of several health insurance options for small employers and uninsured individuals from which to choose.

The biggest challenge currently facing the MSP program is retaining existing Issuers (health care plans) and attracting new Issuers into the program. Participation in the MSP program is voluntary and the uncertainty about the ACA due to the many lawsuits, funding, regulatory environment, multiple oversight agencies, large premium rate increases, and the ongoing volatility in the small group and individual marketplaces continues to stymie OPM's ability to retain current and attract new Issuers. The OIG issued a Management Alert Memo¹ on December 8, 2016, to the Director of OPM to describe the status of MSP program. The memo referenced the fact that until there is individual and small market stabilization, the MSP program will continue to see volatility and a reduction of state-level issuers.

Despite the many challenges, OPM continues to work toward meeting the goal of making MSP program health insurance options available for enrollment by contracting with the Blue Cross Blue Shield Association and an individual Co-Op to offer MSPs in 22 marketplaces in 2017. OPM has also taken steps to clarify, in the future, the MSP naming convention used for the MSP options that are offered on the marketplaces. This may help clarify the consumer's choice of the product.

Additionally, OPM has been diligent in attempting to reach out to insurance companies and working to grow the MSP program. However, despite all of OPM's efforts, the marketplaces remain volatile and there is no ability to estimate how many MSP options might be offered in 2018. To add to the volatility, the Administration recently issued an Executive Order to stop the payment of cost-sharing reductions to the health care plans that are owed money from the Federal Government for services rendered to qualified low-income enrollees. Congress is currently working on legislation that would appropriate the cost-sharing reduction funds, but there is no certainty that the bill would pass both chambers of the legislature. Should this and the other issues currently plaguing the state marketplaces not be resolved, the program could lose its remaining participating issuers, which would have a negative impact on competition and choice for the members who are relying on this program to meet their health care needs.

¹ <https://www.opm.gov/our-inspector-general/reports/2016/management-alert-status-of-the-multi-state-plan-program-4a-hi-00-17-013.pdf>

3. BACKGROUND INVESTIGATIONS

In January 2016, the Administration announced the establishment of the National Background Investigations Bureau (NBIB), which absorbed the majority of the Federal Investigative Services' (FIS) mission, functions, and personnel. The initial operating capability for NBIB occurred on October 1, 2016. However, OPM leadership acknowledges that it will take significantly longer to make the full transition from FIS, NBIB's predecessor organization. The following sections highlight NBIB's challenges and current initiatives in place to address them.

A. National Defense Authorization Act (NDAA) §951

One key challenge faced by the NBIB is uncertainty as to its future responsibilities. Specifically, Congress has been considering for the past two years whether to permit the DOD to conduct its own background investigations.

Last year, Congress passed a provision in the FY 2017 National Defense Authorization Act (NDAA) that directed DOD to prepare a plan to potentially transition a large portion of the background investigations program from OPM to DOD. DOD prepared this plan and presented it to Congress. In September 2017, the Senate passed a version of the NDAA for FY 2018 that contained a provision permitting DOD to implement that plan. This provision was not included in the bill passed by the House of Representatives in July 2017. In late October 2017, the bill went to conference and the differences were not resolved prior to publication of this document.

If Congress allows DOD to re-assume the authority to conduct its own background investigations, NBIB would be faced with the dual challenges of ensuring the efficient transfer of its DOD caseload and servicing its remaining customers with fewer resources.

B. National Background Investigations Bureau

In January 2016, the Administration announced the establishment of the NBIB, which absorbed the Federal Investigative Services' (FIS) background investigation mission, functions, and personnel. NBIB is unique in that it is housed in OPM, but the DOD has been tasked through Executive Order with responsibility for the design, development, security, and operation of NBIB's background investigations IT systems.

There have been a number of developments during NBIB's inaugural year. NBIB expanded both its Federal and contractor workforce by hiring 200 Federal investigators and signing two new background investigations contracts. It also established a cross-agency Backlog Reduction & Mitigation Initiative Working Group to identify ways to

address the background investigation backlog. NBIB is working with DOD's Defense Information Systems Agency to create the new IT system needed to support its operations. OPM informed us that NBIB further secured and modernized its information technology through the development of an eAdjudication prototype. NBIB is currently working to modernize business processes and tools, has in place a new organizational model to bolster security and intergovernmental communications, and utilizes an updated governance structure that will better align policy and operations and facilitate continuous improvements.

The establishment of the NBIB is the most significant institutional reorganization since OPM absorbed DOD's background investigations unit, the Defense Security Service, in 2005. The unique partnership with DOD increases the complexity of this task. Although DOD is responsible for the design and operation of the IT systems, OPM is the system owner and OPM employees and contractors are the end users; therefore, OPM has been, and must continue to be, actively involved in the development and implementation of the systems. Further, this dual agency relationship also requires that the agencies work closely on major administrative issues, such as funding and contracting.

The OIG has been monitoring the agency's progress in transitioning operations from FIS to NBIB, including receiving regular briefings from the NBIB Director and OCIO staff. Although we have not yet conducted any formal audit oversight of NBIB, we included the establishment of this new entity as a management challenge because of the scope and complexity of this massive endeavor. As such, we anticipate that this will continue to be a top management challenge for OPM for at least the next few years.

C. Case Processing Backlog

NBIB is responsible for processing background investigations for Federal applicants, employees, and contractor personnel for customer agencies. NBIB provides investigative reports on the basis of which other agencies, either the employing agency or the agency sponsoring the request for a security clearance or credential, make determinations of various eligibilities.

Under the Intelligence Reform and Terrorism Prevention Act of 2004, guidelines and additional guidance issued by The Security Executive Agent, the fastest 90 percent of initial security clearance investigations should be completed in 40 days, and the fastest 90 percent of initial Top Secret investigations should be completed in 80 days. However, for FY 2017, NBIB failed to meet its timeliness goals by a significant margin. NBIB completed the fastest 90 percent of initial security clearance investigations in 159 days and completed the fastest 90 percent of initial Top Secret investigations in 326 days.

In 2017, NBIB increased the capacity of its background investigator workforce by initiating a new background investigations contract, which increased the workforce from two to four background investigator contractors. Additionally, NBIB:

- Teamed with the four fieldwork contractors and provided them with incentives to build capacity, increase production, and reduce the inventory of aged investigations;
- Hired 200 additional Federal background investigators;
- Concentrated the background investigative workforce in the highest workload locations;
- Began work with a cross-agency Backlog Reduction & Mitigation Initiative Working Group to identify potential initiatives and recommendations that will lead to the reduction of the backlog; and
- Partnered with the 'DOD's Defense Information Security Agency to build a more secure and flexible case management system.

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 has already expended a great deal of resources to meet these challenges, and made some notable improvements, they will need to continue their current 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 clearly 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 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.

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, and our recommendation was that the agency recruit a staff of information security professionals to act as Information System Security Officers (ISSO) that report to the OCIO.

OPM has since centralized its cybersecurity program under a Chief Information Security Officer (CISO) that is supported by a team of ISSOs and network security engineers. This team has developed policies and procedures designed to improve the efficiency with which this team operates, and has implemented a variety of technical security tools and controls that help protect the agency from cyber-attack.

We believe that this centralized security governance structure can be effective, but the ISSO team is currently not effectively fulfilling its responsibilities. While OPM's cybersecurity

posture is notably better than it was in the past, the organization continues to struggle to comply with both traditional and recently implemented FISMA requirements, and is not making notable progress in implementing our FISMA audit recommendations. OPM has only closed 34% of the FISMA findings issued in the past two years, and we expect the number of new recommendations issued to significantly increase as the FISMA audits continue to evolve and look into new areas of the agency's technical operations.

Our FISMA audit reports currently classify OPM's information security governance structure as a significant deficiency, as the agency continues to face challenges in recruiting and maintaining a qualified team of security professionals to manage information system security.

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.

Previous FISMA audits identified a material weakness in OPM's Authorization process related to incomplete, inconsistent, and sub-par work products. OPM resolved the issues by implementing new policies and procedures to standardize the Authorization process. However, throughout FY 2014 and FY 2015, the number of OPM systems without a current and valid Authorization significantly increased, and we reinstated the material weakness related to this issue in our FY 2015 FISMA audit.

In April 2015, OPM's OCIO issued a memorandum that granted an extension of the previous Authorizations for all systems whose Authorization had already expired, and for those scheduled to expire through September 2016. The justification was that OPM was in the process of modernizing its information technology (IT) infrastructure and that once this modernization was completed, all systems would have to receive new Authorizations anyway. We expressed serious concern with this approach, and warned the agency of the extreme risk associated with neglecting the IT security controls of its information systems.

In an effort to revitalize its Authorization program, in FY 2016 OPM initiated an "Authorization Sprint" designed to get all of the agency's systems compliant with the Authorization requirements. OPM dedicated significant resources toward re-Authorizing the systems that were neglected. By the second quarter of FY 2017, the OCIO had completed an Authorization for every major information system owned by the agency, and had successfully addressed some of the critical weaknesses that our audits had identified with the previously completed Authorization packages. As a result of these improvements, we

upgraded the material weakness related to system Authorizations to a significant deficiency. However, we continue to detect widespread issues – albeit less severe – in OPM’s Authorization process. These ongoing issues primarily relate to incomplete or inadequate independent testing of the systems’ security controls.

The OCIO has continued its efforts to implement a comprehensive security control continuous monitoring program that will eventually replace the need for periodic system Authorizations. However, OPM’s continuous monitoring program has not reached the point of maturity where it can effectively replace the Authorization program.

We acknowledge the improvement that OPM has made in its Authorization program, and are optimistic that the agency is on a path toward addressing the significant deficiency and audit recommendations in this area. We will continue to closely monitor this issue going forward.

3. DATA SECURITY

Targeted and advanced attacks on computer networks are becoming increasingly frequent, and IT security professionals are in a race to secure their networks before the next breach occurs.

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. Over the past several years, the agency has increased the staffing levels of its network security team. OPM has also implemented a variety of security tools associated with the Department of Homeland Security’s Continuous Diagnostics and Mitigation program, and these tools help automate efforts to secure the agency’s network. In addition, OPM has made notable progress in encrypting the databases that support the agency’s most sensitive systems. While this control also adds value, encryption in itself does not adequately protect sensitive data, as merely the compromise of a valid user’s password would 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 has 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 the back-end applications were configured to only allow PIV authenticated users, an attacker would have extreme difficulty gaining unauthorized access to data without having physical possession of an authorized user's PIV card.

OPM's FY 2017 Major Management Challenges progress update states that it has enabled multifactor authentication for 53 percent of its major applications. However, these numbers do not accurately reflect the data security posture of the agency, as they inappropriately include systems that require users to first authenticate to the OPM network using a PIV card, but still accept a username and password to gain access to the application itself. Without the enforcement of PIV authentication at the application level, users of the network (either valid users or unauthorized attackers) could still gain access to applications that they are not authorized to use. Our recent audit work indicates that only two major applications enforce multifactor authentication via PIV card at the application level.

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. OPM's efforts in modernizing the agency's ageing IT hardware and applications have not been funded, and the agency has made limited progress in this area.

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, identifies the full scope and cost of the IT modernization and stabilization project. OPM's lack of disciplined project management and capital budgeting processes surrounding the troubled Shell project influenced the decision-making process of the Appropriations committees in Congress that drafted the FY 2017 spending bill. This is clear from our prior reporting on the matter, our interactions with the committees during the drafting process, and the committee report which amplifies the intent of the language. Congress is willing to fund OPM's modernization efforts provided that OPM has developed a clear strategy for the total effort, has identified the technical level of effort involved, and has estimated the total costs of the 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 a United States Office of Management and Budget (OMB) Major IT Business Investment (OMB Exhibit 300). OPM has not yet completed its FY 2017 spending plan or provided any of the associated artifacts.

OPM faces enormous hurdles in reaching its desired outcome of modernizing its legacy infrastructure and applications. OPM must develop a workable strategy and follow established project management and capital budgeting processes to achieve its goals.

5. STOPPING THE FLOW OF IMPROPER PAYMENTS

In FY 2016, OPM paid over \$82 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 make contributions.

In its annual financial report, OPM reported that the overall improper payment rate for these retirement programs was .37 percent in FY 2016. Although this rate is quite low compared to many other Federal programs, the total amount of all types of improper retirement payments reported by the agency was \$304 million. Therefore, under the Improper Payments Elimination and Recovery Act of 2010 and OMB Circular A-123, the retirement programs are considered to be at risk for significant improper payments because the program's improper payments annually total more than \$100 million.

The OIG has spent a decade examining a specific type of improper retirement payment: those made to deceased annuitants. We spend a significant amount of time and resources investigating such cases and regularly find situations where a single deceased annuitant was improperly paid over five, ten, or even twenty years. This is why we have repeatedly advocated for the institution of additional and improved internal controls to monitor annuitant deaths, focusing upon the elderly population.

We have discovered in our years of studying Retirement Services' program integrity operations that the office is woefully understaffed to sufficiently handle the volume of work and to handle the workload associated with validating an annuitant's status.

In addition, we have determined that Retirement Inspections lacks a comprehensive centralized tracking system to record and analyze its program integrity work. This tracking

system would document, store, record, communicate, and report all activities associated with a particular case and support the actions and decisions made by Retirement Services.

The OIG predominately receives suspected fraud referrals resulting from the Retirement Inspections Group's work on the Social Security Death Match. However, we rarely, if ever, see suspected fraud referrals concerning the other program integrity work performed.

One example of Retirement Services' other program integrity work is the marital survey conducted by the Retirement Surveys Group to determine if survivor annuitants under the age of 55 are still eligible to receive a survivor annuity.

During FY 2017, we conducted a pro-active project to examine Retirement Services' work in this area. Our review showed that some of the survivor annuitants had in fact remarried prior to age 55, resulting in a computed overpayment.

We believe that additional unreported remarriages exist, and Retirement Services' failure to identify them results in the continuation of improper payments. Consequently, we suggest that Retirement Services initiate a project to identify unreported marriages.

For years, OPM leadership has failed to prioritize the prevention of improper payments in its budget requests, and as a result, Retirement Services now lacks the resources to adequately perform the work necessary to protect Federal funds from this waste. OPM management has a duty to the American people to protect the integrity of the retirement trust fund from waste from improper payments.

6. RETIREMENT CLAIMS PROCESSING

OPM is responsible for processing retirement applications for Federal employees, and the timely issuance of full annuity payments to annuitants remains a challenge for OPM. In January 2012, the Retirement Services office released and began implementation of its Strategic Plan with the goal of adjudicating 90 percent of retirement cases within 60 days starting in July 2013. A portion of Retirement Services' workload involves retirement benefits provided by other agencies that need to be coordinated with OPM's benefits, such as Federal Employees Retirement System disability benefits and Office of Workers' Compensation Programs claims.

As of FY 2017, Retirement Services has not met its strategic plan goal of adjudicating 90 percent of retirement cases within 60 days. Specifically, the percentage of claims that were processed in 60 days or less decreased from 77 percent in FY 2016 to 57 percent in FY 2017.

In addition, where claims in this category were processed in an average of 40 days in FY 2016, it took Retirement Services 47 days to process a claim in FY 2017.

While Retirement Services has not met its strategic plan goal, the office has decreased the average number of days in which claims over 60 days old were processed from 102 days in FY 2016 to 93 days in FY 2017.

OPM appears to remain focused on its internal process improvements and external outreach towards other Federal agencies to meet their goal set in its 2012 strategic plan of processing 90 percent of claims within 60 days, and continues to implement the core components in the Retirement Services Strategic Plan, including people; productivity and process improvements; partnering with agencies; and partial, progressive IT improvements. OPM also continues to focus on its ongoing Lean Six Sigma efforts.

However, without proper resources, OPM's ability to meet its goal of processing 90 percent of retirement claims in 60 days remains in jeopardy. In addition, if OPM does not receive funding for its IT initiatives, the ability to achieve sustained progress in meeting its processing goals will be severely impacted.

During FY 2017, Retirement Services has taken on the challenge of reducing call waiting time by hiring additional Customer Service Specialists and Legal Administrative Specialists to help with the yearly surge that occurs from February through March. In addition, Retirement Services/Benefits Officers Training and Development (BOTD) delivered a pre-retirement seminar on Capitol Hill to congressional staffers. Retirement Services/BOTD also held two training events where Benefit Officers came from agencies across the Federal government to take part in workshops on Federal Retirement, Insurance, Benefits, and Financial Planning.

7. PROCUREMENT PROCESS FOR BENEFIT PROGRAMS

On October 14, 2015, the OIG issued a Management Alert memorandum to OPM's 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 has corrected some of the deficiencies in its benefit program procurement process and it has strengthened its oversight role in monitoring these procurements. The Office of Procurement Operations (OPO) and Federal Employee Insurance Operations (FEIO) have 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, two of the four recommendations identified in our Management Alert memorandum have been satisfactorily implemented by OPM and closed.

After nearly 13 years, OPM awarded a new FSAFEDS contract on March 1, 2016, to WageWorks. The FSAFEDS program was fully transitioned to WageWorks by the planned date of September 1, 2016. In addition, a new FLTCIP contract was also awarded on April 5, 2016, and the BENEFEDS procurement was awarded on March 15, 2017.

We commend OPM's efforts to correct some of the 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 FEIO 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 the applicable law 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.

8. PROCUREMENT PROCESS OVERSIGHT

OPM's OPO is responsible for providing centralized contract management that supports the operations and Government-wide missions of OPM, as well as managing the 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 current and former Federal employees.

During FY 2017, OPO has continued to work with the Internal Oversight and Compliance office in executing an established corrective action plan to appropriately 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.

Specifically, OPO states that they have taken the following steps during FY 2017 to address the OIG's concerns in the reported areas:

- Resource Levels – Hiring staff at all levels, securing contractor support for critical OCIO IT requirements and agency-wide closeout efforts, and communicating challenges to OPM leadership.
- Delegation of Authority – Finalizing the agency-wide warrant (delegated procurement authority) refresh², and review and approval of drafted Oversight and Compliance Policy (through General Counsel and Labor Relations).
- Customer Communication and Outreach – Continuing (1) procurement action reviews with OPM program offices, (2) collaboration efforts with OMB/ Office of Federal Procurement Policy on their Acquisition 360 initiative, and analyzing FY 2017 survey data to identify improvement opportunities, and (3) to strengthen communication through training and briefing events.
- Standardized Documentation and Updated Policies and Procedures – Issuing new policy and internal guidance related to acquisition planning, Contracting Officer Representatives, and Procurement Request Cut-Off Date and Procurement Action Lead Time.
- Documentation Accessibility – Internal guidance is made available to staff through the OPO’s internal website.
- Staff Training –Holding staff training through internal and external venues.
- Lack of Procurement Actions Oversight and Review - Drafting oversight and compliance policy that will "go-live" at the beginning of FY 2018.

OPO’s continued commitment to actively improve its internal controls is a sign that, although it will take time to implement the necessary corrective actions, improvements are occurring.

² 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.



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