



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Office of the
Inspector General

October 12, 2016

MEMORANDUM FOR BETH F. COBERT

Acting Director

FROM: NORBERT E. VINT
Deputy Inspector General

A handwritten signature in black ink that reads "Norbert E. Vint".

SUBJECT: Fiscal Year 2016 Top Management Challenges

The Reports Consolidation Act of 2000 requires the Inspector General to identify and report annually the top management challenges facing the agency. In meeting this requirement, we have classified the challenges into two key types of issues facing the U.S. Office of Personnel Management (OPM) – environmental challenges, which 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.

The three listed environmental challenges - strategic human capital, Federal health insurance initiatives, and background investigations - facing OPM 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 internal challenges we have identified for this letter represent challenges related to information technology, improper payments, the retirement claims process, and the procurement process.

Inclusion as a top challenge does not mean we consider these items to be material weaknesses. In fact, the area of security assessment and authorization is the only challenge included that is currently a material weakness.

The remaining 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. We have categorized the items included on our list this year as follows:

Environmental Challenges

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

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.

We have identified these 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.

The attachment to this memorandum includes written summaries of each of the challenges that we have noted on our list. These summaries recognize OPM management's efforts to resolve each challenge. This information was obtained through our analysis and updates from senior agency managers so that the most current, complete, and accurate characterization of the challenges are presented.

One of the challenges included in last year's memorandum was removed this year:

- Phased Retirement has been removed from the Strategic Human Capital Management challenge due to OPM's fulfillment of its primary role of providing regulations and

comprehensive guidance to Federal agencies. While there is continued concern regarding the lack of agency and employee awareness of, as well as interest in, the program, especially considering that 31 percent of the Federal workforce is already or will be retirement-eligible by September 2017,¹ the challenge is now on Federal agencies to determine whether or not to implement a phased retirement program.

In addition, we have added the following challenge:

- Background Investigations, as specifically related to the National Background Investigations Bureau transition and Case Processing challenges, has been added because of the need to meet timeliness expectations and increase resources to improve processes and productivity.

I believe that the support of the agency's management is critical to meeting these challenges and will result in a better OPM for our customer agencies, Federal employees, annuitants and their families, and the taxpayers. I also want to assure you that my staff is committed to providing audit or investigative support as appropriate, and that they strive to maintain an excellent working relationship with your managers.

If there are any questions, please feel free to contact me, or have someone from your staff contact Michael R. Esser, Assistant Inspector General for Audits, or Michelle B. Schmitz, Assistant Inspector General for Investigations, at 606-1200.

Attachment

¹Government Accountability Office, January 2014, FEDERAL WORKFORCE Recent Trends in Federal Civilian Employment and Compensation report to the ranking member, Committee on the Budget, U.S. Senate, <http://www.gao.gov/assets/670/660449.pdf>.

**FISCAL YEAR 2016 TOP MANAGEMENT CHALLENGES
U.S. OFFICE OF PERSONNEL MANAGEMENT**

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.

Improving the Federal Recruitment and Hiring Process

Throughout fiscal year (FY) 2016, OPM continued to lead and support the CHCO Council’s formal Executive Steering Committee for skills gaps. The CHCO Council’s Executive Steering Committee is co-chaired by the CHCOs from the Department of Treasury and the National Science Foundation. The Executive Steering Committee 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. With OPM support, the Executive Steering Committee makes key decisions around the design and execution of the Government-wide and agency-specific skills gaps efforts and brings recommendations and updates to the CHCO Council for review and approval. The Executive Steering Committee meets quarterly to formulate plans, review progress, and make key decisions on the design and implementation of skills gaps efforts across the Federal Government.

Upon identifying the Government-wide and agency-specific Mission Critical Occupations, which was done in FY 2015, work then began to identify and establish the Federal Action Skill Teams responsible for leading the effort to: (1) identify root causes of skills gaps in the occupations; (2) develop strategies to address prioritized root causes; (3) establish goals and outcome-oriented metrics; (4) document action plans to address skills gaps; and (5) submit quarterly updates to OPM to monitor progress on executing action plans and achieving metric targets.

The Government-wide Federal Action Skill Teams are being led by occupational leaders, who are respected senior (technical) subject matter experts representing each of the Government-wide Mission Critical Occupations. The occupational leaders are partnered with a CHCO to serve as a technical Human Resources (HR) lead to provide guidance for how to apply human resources policies and strategies. Additionally, CHCOs are responsible for leading the Federal Action Skill Teams within their respective agencies.

During 2016, OPM conducted four in-person training sessions and one virtual training session for field personnel regarding the root cause analysis and strategy development and implementation process for the Federal Action Skill Teams. Throughout the entire process, OPM, in coordination with the Executive Steering Committee, provides on-going support and technical guidance to agencies and the occupational leaders.

Concurrently, OPM, in coordination with the Office of Management and Budget (OMB), published the proposed rule for revising Title 5, Code of Federal Regulations, Part 250. The regulation promulgates skills gaps and requires agencies to:

- Make progress toward closing any knowledge, skill, and competency gaps;
- Use the OPM designated method to identify skill gaps;
- Monitor and address skill gaps within Government-wide and agency Mission Critical Occupations;
- Describe the skills and human capital information required to achieve agency goals and objectives, within agency strategic plans; and
- Include explicit descriptions of agency skills and competency gaps that must be closed, within annual Human Capital Operation Plans.

OPM has had success in creating an infrastructure and governance structure for closing 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. OPM obtained agency tools and information from data requests to the CHCO Council and Chief Learning Officers Council to complete planned actions leading to the many accomplishments and outcomes for FY 2016. By the end of FY 2016, a proposed Delegated Examining Certification program of competence will be presented to the Executive Steering Committee for closing HR skills gaps.

Federal hiring, specifically closing mission-critical skills gaps, continues to be a concern Government-wide, and while OPM has made progress in working to close the skills gaps within the Federal Government, the implementation of targeted goals is still ongoing.

2. FEDERAL HEALTH INSURANCE INITIATIVES

Two major challenges for OPM involve the Federal Employees Health Benefits Program (FEHBP) and the Multi-state Program Plan (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 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, the average FEHBP premium increase for Federal employees and retirees is 4.4 percent, which is down 2 percentage points from the 2016 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 the 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 ensure that the system remains secure 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 on pages 17-19 of this memo).

2) Prescription Drug Benefits and Costs

The financial cost of health care in the United States (U.S.) continues to rise, with most industry experts agreeing this trend will continue for years to come. It is reported that by the year 2021 health care costs will reach \$4.8 trillion in the U.S. alone, up from \$2.6 trillion in 2010. Currently, health care represents approximately 20 percent of our country's Gross National Product. Prescription drugs are a significant portion of this cost and will likely continue to become a larger component of health care costs as more pharmaceutical advancements are discovered and new biotechnology/biosimilar agents enter the market. OPM must develop an effective, long-term strategy to mitigate and manage FEHBP prescription drug costs while maintaining overall program value.

One opportunity to lower prescription drug costs that OPM should give serious consideration to is carving out the pharmacy benefit entirely from the health benefits

currently provided by FEHBP fee-for-service, experience-rated, and community-rated carriers. This would allow OPM to gain more control over its prescription drug program and improve cost and utilization containment efforts. Since the inception of the FEHBP, pharmacy benefits have been offered through 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 leveraging the purchasing power of over 8 million FEHBP members to negotiate a single the PBM contract with OPM, the FEHBP pharmacy costs vary greatly and are fragmented among the hundreds of participating carriers. Furthermore, since OPM has no 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 provide OPM with added transparency, more favorable contract terms, customized clinical programs that best fit the FEHBP's health care utilization, and may provide greater rebates and lower pharmacy cost for the FEHBP.

In 2011, "The President's Plan for Economic Growth and Deficit Reduction" called 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. Because current FEHBP law precludes OPM from contracting directly with PBMs, OPM has proposed statutory authority language changes, seeking to amend the current FEHBP law to permit OPM to contract directly with PBMs. However, this proposal has languished, and there has not been a concentrated effort by OPM to push this initiative to Congress for approval.

OPM has and continues to emphasize ways to ensure effective uses of prescription medications to manage drug costs through calling on participating health plans to:

- Better manage formularies and pharmacy networks;
- Implement, operate, and reinforce drug utilization management strategies;
- Limit reimbursement of specialty drugs to the pharmacy benefit;
- Offer a prescription drug benefit that includes at least four tiers; and
- Implement a cost comparison tool that gives current and prospective enrollees access to user friendly information about the formulary tier and member cost-share for prescription drugs.

We recognize and applaud the agency's efforts thus far and we are confident that they will have a positive impact on the program. But, we continue to encourage OPM to work with its Office of Congressional and Legislative Affairs to make the proposed statutory authority language change a priority initiative to advance to Congress for its

approval. Allowing OPM to have direct contracting authority with PBMs will provide the FEHBP stronger purchasing power, help to ensure that the benefits and fees negotiated are in the best interests of the FEHBP, and will strengthen the controls and oversight of the FEHBP pharmacy program.

We agree with OPM that a detailed study should be undertaken to carefully weigh the positive and negative implications of contracting directly with a PBM. OPM has committed to including such a study in its future plans.

Ultimately, any changes implemented to the FEHBP's pharmacy benefits will need to meet the challenge of ensuring that the changes do not adversely impact FEHBP enrollees' health and safety while realizing true program savings.

3) Health Benefits Carriers' Fraud and Abuse Programs

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 Office of the Inspector General (OIG). At a minimum, FEHBP carriers are required to implement programs to:

- Proactively identify FWA issues, identify program vulnerabilities, initiate action to deny or suspend payments where there is potential FWA, develop and refer cases to the OIG for consideration of civil and criminal prosecution and/or application of administrative sanctions, and provide outreach to providers and beneficiaries;
- Conduct investigations of FWA allegations referred by internal or external sources;
- Maintain a case tracking system of all FWA cases opened, active, pending, and closed;
- Provide claims data to the OIG upon request;
- Provide liaison and investigative support to the OIG and other law enforcement agencies;
- Track all member, provider, and pharmacy case notifications sent to the OIG; and
- Provide annual FWA reports (medical and pharmacy) to OPM.

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

Recent OIG audits have shown that health carriers have not appropriately reported fraud and abuse cases to OPM and the OIG, and some carriers have not implemented procedures to address fraud and abuse issues in their pharmacy programs. Specifically, the reporting of quality FWA cases, as well as underreporting or untimely reporting of cases to the OIG, continue to be significant issues with the FEHBP carriers. Furthermore, carriers continue to be challenged with providing accurate and complete data within the required FWA annual report.

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 drafted and issued a new Carrier Letter to all FEHBP carriers. Carrier Letter 2014-29 has new definitions, training guidance, and updated reporting requirements. The new Carrier Letter also requires carrier management to certify to the completeness and accuracy of the fraud and abuse information submitted on the annual report.

However, after reviewing the 2015 fraud and abuse reports submitted under the new Carrier Letter, 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. During FY 2016, there has been a significant increase in the number of case notifications (a record number of over 3,000 cases) received from the carriers. This is a direct result of our audit work and the collaboration with OPM. While the quantity of these notifications has increased dramatically, the carriers still require guidance on submitting *quality* referrals. Also, of continued concern, we determined that less than 30 percent of the carriers' FWA cases opened with FEHBP exposure in 2015 were actually reported to the OIG.

As a result of recent OIG audits, OPM has reviewed its practices and procedures and implemented changes to strengthen its existing FWA monitoring and enforcement. During the past year, OPM has continued to:

- Partner with the OIG to resolve open fraud-related audit recommendations.
- Meet with the OIG to review and discuss the annual reports received from the carriers.

OPM agrees that more work needs to be done. Their next steps include:

- Analyzing carrier reports to get a better understanding of carriers' fraud and abuse programs, and to determine if carriers need further guidance for the reporting requirements;
- Exploring changes to the annual report and expectations of the carriers; and
- Providing a better understanding of the reporting requirements to the carriers.

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 carriers accountable for operating effective fraud and abuse programs. Now that better, more comprehensive guidance has been issued, OPM needs to enforce these requirements and hold 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. The FEHBP MLR methodology is closely monitored by OPM's Office of the Actuaries. For each non-traditional community-rated FEHBP plan, the Office of the Actuaries documents each year's MLR and the associated penalties or credits in a formal letter. The underlying data used in the letter is kept in a secure proprietary database so the following year's letter will reference any remaining credit.

The 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 unique situations to the FEHBP MLR surface, the need for detailed criteria and carrier instruction is vital. During recent MLR audits, the OIG identified new areas of the MLR methodology that lack clear instructions from OPM. 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, in some instances this is not

feasible or even applicable. While 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, 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.

Specifically, recent audits have identified concerns regarding Federal income tax allocation methods and the use of global capitations as claims cost in the MLR calculation that are in need of FEHBP-specific guidance. 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.

Another pressing issue experienced on MLR audits is the large variances between OPM's subscription income reports and the FEHBP premiums carriers track in their systems. The MLR rules state that carriers can choose to use their own premium numbers in the MLR calculation, but the carrier premiums will be subject to audit if used. Therefore, most carriers use OPM's subscription income amounts as the denominator in the MLR formula instead of their own premium numbers. However, carriers have continued to express frustration with OPM's inability to support the accuracy of the subscription income numbers. OPM's subscription income amounts are unsupportable and have been for decades due to the decentralized enrollment and payroll systems. Consequently, OPM's intention is to allow this choice for the foreseeable future. While we understand the complexities that come with a decentralized enrollment and payroll system, OPM still has a fiduciary responsibility to ensure that the subscription income amounts it reports are as precise as they can be. As the methodology currently being used to derive these amounts is unsupportable, it is incumbent upon OPM to consider replacing the current methodology with one that will produce more accurate results. Otherwise, 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 options. 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 (MSP) will be one of several health insurance options for small employers and uninsured individuals from which to choose.

While implementing any new program represents a host of complex challenges, one continuing challenge is securing sufficient resources for OPM's MSP program function, since the ACA does not specifically fund OPM for this new health care responsibility and prohibits the use of FEHBP resources to manage the MSP program.

An even greater challenge, however, 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, 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.

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 two individual Co-Ops (a non-profit organization in which the same people who own the company are insured by the company) to offer MSPs in 33 marketplaces in 2016;
- Continuing to develop relationships with state health care regulators to facilitate the exchange of information on MSP program operations and various state requirements to sell insurance products in that state;
- Sponsoring an MSP Issuer Conference in November 2015;
- Conducting outreach efforts to insurance Issuers and other groups to raise awareness and potential participation in the MSP program;
- Continuing to work with OMB and HHS to develop standard operating procedures for collecting the MSP user fee;
- Compiling and transmitting information on each applicable state-level Issuer to HHS for the Federally Facilitated Marketplace, to states that intend to operate their own exchange but utilize the prescribed HHS templates, and directly to those states who operate their own marketplace; and
- Establishing an MSP Program Advisory Board to exchange information, ideas, and recommendations regarding the administration of the MSP program.

OPM continues to reach out to insurance companies and is diligently working to grow the MSP program; however, despite all OPM's efforts, only 24 MSPs will be offered in 2017. As discussed and evidenced by the number of MSPs in 2017, the ongoing volatility and current market conditions makes growing the MSP program an increasingly difficult task, which will require OPM to closely monitor the situation, adjust plans as necessary, and keep appropriate parties informed of the ever-evolving situation.

3. BACKGROUND INVESTIGATIONS

The newly established National Background Investigations Bureau (NBIB) and the case processing backlog are two major challenges that may affect the timely completion of background investigations. The following sections highlight these challenges and current initiatives in place to address them.

A. National Background Investigations Bureau

In January 2016, the Administration announced the establishment of the NBIB, which will absorb Federal Investigative Services' (FIS) mission, functions, and personnel. The NBIB is a unique entity in that it is housed in OPM, but the U.S. Department of Defense (DOD) has been tasked with responsibility for the design, development, security, and operation of NBIB's background investigations IT systems. The initial operating capability for NBIB occurred on October 1, 2016, though OPM leadership acknowledged that it will take significantly longer to make the full transition from FIS, which is NBIB's predecessor organization.

The establishment of the NBIB is the most significant institutional reorganization since OPM absorbed DOD's background investigations unit, Defense Security Service, in 2005. The Administration established a Transition Team to spearhead the transfer of FIS's functions to the NBIB. In mid and late September, the agency provided the OIG with some of the necessary institutional establishment documents; however, many of the documents are not yet final. As a result, we are currently unable to assess the quantum of meaningful changes that were made by the target date of October 1, 2016.

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 must 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.

B. Case Processing Backlog

FIS was responsible for processing approximately 2.2 million background investigations per year for Federal applicants, employees, and contractor personnel for customer agencies. FIS determined the eligibility of these individuals to hold security clearances, or to be employed in positions with national security sensitivity, eligibility for accession or retention in the Armed Forces, eligibility for an identity credential, or suitability or fitness for employment for or on behalf of the Government.

FIS's total background investigation backlog as of September 5, 2016, was 569,000 cases. This included all open cases currently pending in their inventory. Based on capacity, their target inventory is between 160,000 – 180,000 cases. 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 fiscal year 2016, OPM failed to meet its timeliness goals by a significant margin. OPM completed the fastest 90 percent of initial security clearance investigations in 105 days and completed the fastest 90 percent of initial Top Secret investigations in 214 days.

There were two key events that resulted in the backlog of cases:

- The first event was the termination of the US Investigations Services, LLC fieldwork contract that led to several hundred contractor background investigators leaving the industry. KeyPoint and CACI, the remaining two FIS contractors, hired approximately 1,600 new field background investigators and during the same period they lost over 1,200 staff through attrition. Current industry background investigations capacity falls well short of meeting customer demands.
- The second event was funding shortfalls which have significantly impacted FIS's ability to grow the Federal and contractor capacity and work overtime to address the backlog.

A plan of action to reduce the number of cases to a manageable level has been developed. The following capacity growth initiatives and process efficiencies are currently being implemented to help address the growing backlog challenge:

- Increase investigative capacity through the hiring of both additional Federal staff and increased contractor production.

- Implement process efficiencies to reduce total man-hours to complete ongoing work.

Furthermore, OPM has recently awarded four new fieldwork contracts to companies that will work with NBIB to provide background investigations for Federal agencies. The challenge associated with reduced capacity has been exacerbated by the inaccurate workload projections provided by FIS's customers. In FY 2016, agency workload projections were underestimated by 22 percent, further complicating FIS's ability to accurately predict and address background investigative workloads. For fiscal year 2017, process efficiencies to reduce total man-hours to complete ongoing work will also be put in place.

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, 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 reports to the OCIO.

Our FY 2014 FISMA report reduced the severity of the material weakness to a significant deficiency based on OPM's plan to fill enough positions to manage the security for all OPM information systems. In FY 2015, OPM successfully filled the vacant ISSO positions, effectively centralizing IT security responsibility under the Chief Information Officer and fulfilling our audit recommendation. With this new governance structure in place, we closed the audit recommendation related to security management and removed the significant deficiency from our report.

However, our current FISMA audit work has indicated a significant regression in OPM's compliance with FISMA requirements, as the agency is failing to meet requirements that it had successfully met in prior years. In addition, OPM has only closed 46 percent of the FISMA findings issued in the past two years. We believe that this is a security governance issue, as significant responsibility for implementing many FISMA requirements lies with the ISSO function.

We continue to believe that the existing centralized security governance structure *can* be effective, but the ISSO team was severely understaffed throughout the majority of FY 2016. The OCIO lost over half of the ISSOs that were in place at the time we removed the significant deficiency from our report. The OCIO has recently hired additional ISSOs, but these individuals have not yet had the opportunity to be effective in implementing FISMA requirements and address outstanding audit recommendations. OPM continues to face a significant challenge 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 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.

Although the moratorium on Authorizations has since been lifted, the effects of the April 2015 memorandum continue to have a significant negative impact on the agency. The infrastructure modernization project was suspended as the agency re-evaluates its approach,

and many of the systems included in the memorandum continue to operate in the same legacy environment without a valid Authorization. An “Authorization Sprint” in FY 2016 was successful in completing new Authorizations for six systems. However, at the end of FY 2016, there were still 16 major information systems operating without a valid Authorization.

The OCIO is working 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. In addition, OPM acknowledges that a current and comprehensive Authorization for each system is a prerequisite for a continuous monitoring program, as the Authorization will provide a baseline of the security controls that need be continuously monitored going forward.

While we acknowledge OPM’s intent and efforts to address this issue, we believe that the volume and sensitivity of OPM systems that are currently operating without an active Authorization continues to represent a material weakness in the internal control structure of the agency's IT security program.

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, and has procured a variety of tools to help automate efforts to secure the OPM network. However, our FY 2015 FISMA audit determined that not all of these tools were being utilized to their fullest capacity, as the agency was having difficulty implementing and enforcing the new controls in this decentralized infrastructure.

OPM continues to implement additional security tools to further secure its network and data. We agree that these tools add value, but OPM faces the challenge of implementing them into a fragmented environment and fully leveraging their capabilities. OPM has also begun encrypting the databases that support its 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 made progress in requiring the use of PIV authentication to connect an OPM-issued device to the network. However, this control in itself is not sufficient, as users or attackers 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 2016 Major Management Challenges progress update states that it has "enabled multifactor authentication for 71.73 percent of applications and enforced the multifactor authentication on 26.08 percent of systems." However, these numbers are not accurate, 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 one major application (a system owned by the OIG and operated by a cloud service provider) enforces multifactor authentication via PIV card at the application level.

4. INFORMATION TECHNOLOGY INFRASTRUCTURE IMPROVEMENT PROJECT

In the wake of 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. While we agree in principle that OPM's outdated technical infrastructure needs to be modernized, we have serious concerns with the way in which this project was initiated and the way it was managed throughout FY 2016 (see our audit reports on this issue).²

² Flash Audit Alert - U.S. Office of Personnel Management's Infrastructure Improvement Project, <https://www.opm.gov/our-inspector-general/reports/2015/flash-audit-alert-us-office-of-personnel-managements-infrastructure-improvement-project-4a-ci-00-15-055.pdf>; Interim Status Report on OPM's Responses to the Flash Audit Alert – U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project, <https://www.opm.gov/our-inspector-general/special-reports-and-reviews/interim-status-report-on-opm-responses-to-the-flash-audit-alert.pdf>; and Second Interim Status Report on the U.S. Office of Personnel Management's (OPM) Infrastructure Improvement Project – Major IT Business Case, <https://www.opm.gov/our-inspector-general/reports/2016/second-interim-status->

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 suspended the entire project before a single application was modernized and migrated.

OPM is now in the early stages of assessing the alternate solutions that could address the agency's long term technical needs. However, OPM faces enormous hurdles in reaching its desired outcome - many of which we do not believe the agency is adequately prepared to address. OPM has a history of troubled information system development projects. Despite multiple attempts and hundreds of millions of dollars invested, OPM has encountered well publicized failures to modernize its retirement claims processing system. OPM has also faced struggles in modernizing its financial systems and its applications supporting the background investigation process. These are just three specific examples of troubled individual system development projects at OPM. The current initiative, however, will be far more complex than anything the agency has attempted in the past. OPM has dozens of major information systems and hundreds of minor applications that must all be migrated into a new technical environment.

The first major challenge is that OPM does not have a mature program in place to maintain a comprehensive, current, and accurate information system inventory. OPM currently has several initiatives underway to improve its hardware and software inventory management program. The agency has recently made progress developing a list of its servers and databases, and uses an inventory management tool to track the software that is installed throughout the network. However, lists of servers, databases, and software are only partial elements of a complete system inventory. The various elements of an inventory must be mapped to each other so that OPM can accurately define the boundaries of its information systems. OPM still has significant work ahead in converting the raw data it has collected into a comprehensive and mature system inventory.

The second challenge is OPM's lack of dedicated funding to support this project. OPM does not have even general estimates of how much this project will ultimately cost. The agency has requested dedicated funding for technology modernization, but does not have a proper business case or adequate plans to support its request.

The third major challenge relates to the complexity of migrating old information systems into a new environment. Many of OPM's systems are supported by legacy technology that will

not be compatible with a modern technical infrastructure. These systems must be completely redesigned and rebuilt before they can be migrated into a new secure environment. OPM is in the process of developing a digital services team that leverages system development experts throughout government, but simply having development talent available does not resolve the other challenges outlined above.

While we fully support OPM's efforts to modernize its IT environment, we are concerned that there is a high risk that its efforts will ultimately be unsuccessful.

5. STOPPING THE FLOW OF IMPROPER PAYMENTS

Reducing improper payments by Federal agencies continues to be a top priority of both the Administration and Congress. Between 2009 and the present, the Federal Government has built a robust infrastructure of legislative and administrative requirements with which agencies must comply in order to achieve tangible results, most notably Office of Management and Budget (OMB) Circular A-123, Appendix C. OMB released M-15-02, Appendix C, *Requirements for Effective Estimation and Remediation of Improper Payments*, to Circular No. A-123 on October 20, 2014, with significant changes to the policy that oversees how agencies track, report, and oversee improper payments.

Despite these changes, the improper payment of retirement benefits, specifically those to deceased annuitants, continues to be a significant problem at OPM. The retirement programs operated by OPM continue to meet OMB's definition of programs susceptible to significant improper payments because their annual improper payments are over \$100 million per year. Indeed, the improper payments made to deceased annuitants alone regularly total over \$100 million. Between FY 2011, when we first included this issue as a management challenge, and FY 2015, OPM has paid out over \$550 million to deceased annuitants.

We acknowledge that OPM's recapture rate for these improper payments has improved and they recover a large amount of these funds through the Department of the Treasury's reclamation process. However, the fact that they continue to make over \$100 million of improper payments each year is a serious problem and indicates that there are still significant deficiencies in the internal controls designed to prevent improper payments from being paid in the first place. Moreover, an internal OIG analysis identified hundreds of instances where OPM identified a deceased annuitant, stopped the annuity, but failed to reclaim the millions of dollars it had already improperly paid.

Over the years, OPM has initiated a number of projects designed to help mitigate the problem of improper payments to deceased annuitants. During FY 2016, the agency worked to finalize a new Information Exchange Agreement with the Social Security Administration

(SSA). This agreement will hopefully improve the accuracy of data held by both agencies by authorizing OPM to provide SSA with recurring death information from the annuity roll. OPM is currently in discussions with the U.S. Department of Labor's Office of Workers' Compensation Program to establish a similar, mutually beneficial information sharing agreement. We believe that this focus on improving the quality of the data held not only by OPM but also other Federal agencies is a positive development.

The OIG has consistently maintained that the agency does not utilize data mining as a means to identify and prevent improper payments. In response, the agency recently provided us with a list of approximately 30 different reports that it now runs, asserting that use of those reports constitutes data mining within the meaning of our past recommendations. However, despite requests, the agency has failed to provide descriptions of the reports and how they are used. Effective data mining consists of more than simply compiling data. The purpose of such an exercise is to then analyze and use this data to continually evaluate what prevention and identification tools are effective and efficient.

We continue to believe that a key problem with OPM's identification and prevention efforts is that they rarely require an annuitant to actively engage with the agency. Almost all benefit payments are deposited directly into annuitants' bank accounts through electronic funds transfer. OPM routinely sends mail to annuitants, such as information on new cost of living adjustments or changes in the FEHBP, but these mailings do not require any action by the annuitant. Although OPM does send biannual surveys to certain types of annuitants (such as those with representative payees), large segments of the elderly annuitant population do not receive these surveys. OPM proactively reaches out to older annuitants only through special projects conducted on an intermittent basis or if the agency has a specific reason to suspect an annuitant is deceased.

In response to our concerns, OPM will initiate such a special project during the course of FYs 2017 and 2018. The agency is planning to survey annuitants over the age of 90, something that has not been done since 2010. We are encouraged that the agency leadership is finally committing resources to conducting this exercise again.

Despite these modest improvements, we continue to believe that the agency's improper payments prevention program still contains significant deficiencies. The agency does not have a comprehensive strategy in place and without one, they cannot effectively use the information gathered through their various special projects to build a robust set of internal controls to protect the integrity of the retirement programs.

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, 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 August 2016, Retirement Services has not met its strategic plan goal of adjudicating 90 percent of retirement cases within 60 days. Specifically, 78 percent of claims 60 days old or less were processed in an average of 42 days, while claims over 60 days old were processed in an average of 112 days.

OPM is focused on both 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; as well as 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 is 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.

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 procurement operations for several OPM benefit programs. Specifically, these benefit program procurements included the BENEFEDS benefits portal, the Federal Long Term Care Insurance Program (FLTCIP), and the Federal Flexible Spending Account Program (FSAFEDS). The memorandum described the continual delays in OPM's benefit program procurements and the failure to properly manage the bid process for these contracts within the allotted timeframes established by the Federal Acquisition Regulations (FAR). These issues were previously identified and

communicated by our office over several years without a sufficient response or corrective action plan from OPM.

Our primary concern is that the Federal Government, its program participants, and ultimately the American taxpayer may not be receiving the best value in services and benefits because the competitive bidding process has been circumvented or delayed. These delays can be directly associated with a lack of contract oversight by OPM's Office of Procurement Operations (OPO) and the Federal Employee Insurance Operations (FEIO) office's desire for program continuity overriding its responsibility to ensure contracts are re-bid in accordance with the FAR.

Since the issuance of our Management Alert memorandum, OPM has worked to correct the deficiencies in its benefit program procurement process. OPO and FEIO have collaboratively prepared a corrective action plan addressing the OIG's recommendations found in the Management Alert memorandum. The corrective action plan highlights OPM's strategy to:

- Develop and modify existing policies and procedures to improve controls;
- Identify and document roles and responsibilities within OPM offices (including an oversight and compliance process of program offices with delegated procurement authority);
- Assess the feasibility of separating the contracting functions from the administrative functions for FEIO's Healthcare and Insurance group based on overall impact to customers;
- Improve inter-agency procurement communications by conducting monthly meetings with program offices regarding procurement activities;
- Issue quality contracting work file guidance;
- Hire additional operational contract specialists, experienced procurement analysts and cost and pricing analysts;
- Establish a Contract Review Board to ensure oversight and compliance controls of the procurement process; and
- Conduct bi-weekly status update meetings with the OIG to ensure the procurement process for the aforementioned programs remained on target for an award date.

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. A new FLTCIP contract was also awarded on April 5, 2016. The BENEFEDS procurement is currently in progress with an FY 2017 anticipated award date.

While we recognize the above actions are a step in the right direction, the question remains if the corrective action plan is adequate in preventing delays in the procurement process. The challenge for OPM 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. 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, demonstrate compliance with the FAR for the exercise of options, and be documented and approved by OPM's oversight authority (i.e., Contract Review Board). The OIG will continue to monitor the progress of OPM's benefit programs procurement process as it completes this current round and prepares for future procurement actions.

8. PROCUREMENT PROCESS OVERSIGHT

OPM's Office of Procurement Operations 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. Recent internal events, such as the 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 2016, OPO began developing and implementing a corrective action plan to address issues with achieving appropriate resource levels, the lack of delegation of authority oversight, improving customer satisfaction, the lack of standardized documentation and outdated policies and procedures, documentation inaccessibility, outdated training policy, and the lack of procurement actions oversight, as identified in an FY 2015 independent strategic assessment, as well as a recent risk assessment and audit by our office of OPO's procurement operations.

Specifically, OPO has taken the following steps during FY 2016 to address the concerns:

- Resource Levels – OPO performed a review of OMB Benchmarking results for similarly situated contracting offices to assess performance and staffing, and the creation and filling of six new senior positions to support procurement policy development and compliance/oversight functions. In addition, OPO requested and received approval for 11 additional hires over previously approved staffing levels, and has been working with a contractor to obtain additional contract file and contract closeout support.

- Delegation of Authority - OPO developed and issued new policy on Contracting Officer Warrants and has continued ongoing efforts to better understand roles and responsibilities associated with delegated offices' contract administration functions, by collaborating with OPM's Healthcare and Insurance and Employee Services program offices to review Healthcare and Insurance employees' contracts administration functions. In addition, OPO is currently collaborating with Healthcare and Insurance to initiate oversight efforts of delegated procurement actions and commence an initial file review and compliance check process based on existing policy/guidance.
- Customer Satisfaction - OPO worked to distribute surveys to the contracting office, program offices, and vendors, as part of the OMB/Office of Federal Procurement Policy Acquisition 360 initiative, to increase collaboration, provide data on how OPO is doing, and identify opportunities to improve.
- Lack of Standardized Documentation and Outdated Policies and Procedures – OPO also developed and issued new/updated policy and internal guidance related to proper file documentation and maintenance; interim Review and Approval of Contractual Documents, including the Office of General Counsel's role in the contract lifecycle; Contracting Officer Warrants; Category Management; Contract Review Board; update of the Office of Federal Procurement Policy, Small Business Administration Memorandum; Purchase Card Transaction Review; IT Provisions; Acquisition Circular 05-85 and 05-88; Suspension and Debarment; and Ratification of Unauthorized Commitments.
- Documentation Accessibility – OPO's internal policies and guidance are made available to staff through the OPO's internal website.
- Staff Training - OPO held staff training to address the areas of Interim Review and Approval of Contractual Documents, Small Business Subcontracting (in collaboration with the Office of Small and Disadvantaged Business Utilization), Program Office Source Selection, Contracting Officer Warrants, Contract Review Board and the Procurement Information System for Management, and is currently conducting a training and certification assessment of all acquisition professionals in OPM, to include a refresher of Contracting Officer Warrants through the Federal Acquisition Institute Training Application System tool.
- Lack of Procurement Actions Oversight and Review - OPO has started monthly program reviews with all program offices to review all current and planned procurement actions.

While OPO has begun making strides in improving its internal controls, it will take time to determine if the implementation of their corrective action plan leads to improvements in OPO's resource levels, delegation of authority, customer communication, policy

standardization, documentation accessibility, staff training, and procurement actions oversight.