UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

October 27, 2010

MEMORANDUM FOR JOHN BERRY
Director

FROM: PATRICK E. McFARLAND
Inspector General

SUBJECT: 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. We have divided 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 which may be long-term or even permanent; and internal challenges, which OPM has more control over and which once fully implemented will likely be removed as a management challenge.

The three listed environmental challenges facing OPM are due to such things as increased globalization, rapid technological advances, shifting demographics, national security threats and various quality of life considerations that are prompting fundamental changes in the way the Federal Government operates. Some of these challenges involve core functions of OPM that are effected by constantly changing ways of doing business or new ideas, while in other cases they are global challenges every agency has to deal with.

The three internal challenges included in this letter represent OPM's development of new information systems, the need to strengthen controls over its information security governance, and the internal controls over financial management reporting for the revolving fund and salaries and expenses accounts.

Inclusion as a top challenge does not mean we consider these items to be material weaknesses. In fact, the areas of Background Investigations (as part of the Revolving Fund material weakness reported in the Office of the Inspector General's Federal Managers' Financial Integrity Act Management Assurance letter) and Information Security Governance are the only challenges related to reported material weaknesses. The remaining challenges are issues which demand significant attention, effort, and skill from OPM in order to be successfully addressed. However, 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;
- Federal Health Insurance Initiatives; and,
- Background Investigations.

Internal Challenges

- Information System Development;
- Information Security Governance; and,
- Financial Management System and Internal Controls: Revolving Fund and Salaries and Expenses Accounts.

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 the President's Initiatives; 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 is presented. I would also like to point out that we have removed the challenges shown below that were on this list last year:

- Wellness and Work-Life Balance has been removed from the list based on the successful development of wellness programs for the Federal workforce.
- Homeland Security Presidential Directive 12-Personal Identification Verification II has been removed from the list based on the satisfactory progress demonstrated by OPM in meeting the requirements under the directive in providing for secure and reliable forms of identification for Federal employees and contractors.

This year, we have modified and expanded last years challenge concerning the Federal Employees Health Benefits Program (FEHBP). The FEHBP is now a sub-category of the new challenge titled Federal Health Insurance Initiatives. Also included in this challenge is OPM's new role in the national healthcare operations. In addition, we have a new

challenge regarding OPM's Information System Development. This challenge includes sub-categories for the previously reported Retirement Systems Modernization (RSM) and, new for this year, Consolidated Business Information System (CBIS) and Service Credit.

I believe that the support of the agency's management is critical to meeting these challenges and will result in a better government for the American people. I want to assure you that my staff is committed to providing any audit or investigative support needed and that they strive to maintain an excellent working relationship with your managers.

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

Attachment

FISCAL YEAR 2010 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) because of their dynamic, ever-evolving nature, and because they are mission-critical programs.

1. STRATEGIC HUMAN CAPITAL

OPM is the Federal Government's human resource management agency, and is responsible for the strategic management of human capital for the Federal workforce. This includes ensuring that the Federal workforce is managed effectively and efficiently. The strategic management of human capital has been reported as a Government Accountability Office high risk area since fiscal year (FY) 2001. It remained a high risk area in FY 2009 because of a need for a government-wide framework to bring about human capital reform.

In May 2010, President Obama issued a Memorandum, Improving the Federal Recruitment and Hiring Process, beginning the Administration's comprehensive government-wide initiative to address major, long-standing impediments to recruiting and hiring the best and the brightest into the Federal civilian workforce. OPM was directed to:

- Design a government-wide plan for recruiting and hiring qualified, diverse talent;
- Review the Federal Career Intern Program and, within 90 days, offer a recommendation to the President on its future and on providing effective pathways into the Federal service for college students and graduates;
- Evaluate the effectiveness of shared registers used to fill positions common across multiple agencies and improve agencies use of these shared registers;
- Develop a plan to increase the capacity of USAJOBS to provide applicants, hiring managers, and human resource professionals with information to improve the recruitment and hiring process; and,
- Work with agencies to ensure that best practices are being developed and used throughout government.

OPM is charged with leading the way to address and meet the Administration's Hiring Reform initiatives. The best performing organizations focus on people as their most important tool for improving performance. The Federal Government must do the same. OPM is challenged with providing strategic leadership in this effort and providing agencies a full range of support to help them meet the President's ambitious recruitment and hiring reform objectives.

2. FEDERAL HEALTH INSURANCE INITIATIVES

OPM continues to face challenges it must address in order to ensure the FEHBP contracts with insurance carriers that offer comprehensive health care benefits at a fair price. However, with the passing of the Patient Protection and Affordable Care Act (PPACA), OPM's roles and responsibilities related to Federal health insurance have been expanded significantly. Under PPACA, OPM has been designated as the agency responsible for implementing and overseeing the multi-state plan options which start in 2014. More recently, the Department of Health and Human Services reached out to OPM to administer the Pre-Existing Condition Insurance Plan (PCIP). The following highlights these challenges and current initiatives in place to address them.

A. Federal Employees Health Benefits Program

The ever-increasing cost of health care is a national challenge. For the upcoming year, the average FEHBP premium increase is 7.2 percent. While significant, this is less than projected premium increases for other employee-sponsored health care programs, which industry experts estimate will run between 8.9 and 10.5 percent.

As the administrator of the FEHBP, OPM has responsibility for negotiating contracts with insurance carriers covering the benefits provided and premium rates charged to approximately eight million Federal employees, retirees, and their families. The FEHBP must utilize industry best practices and ensure quality healthcare for enrollees while controlling costs. This includes exploring creative ways to control costs and utilization of benefits, such as increased use of wellness initiatives and global purchasing of pharmacy benefits. These challenges may require legislative, regulatory, procurement & contracting, and administrative changes.

OPM believes that the following initiatives will help ensure that the FEHBP continues to offer enrollees quality health care services at fair and reasonable premium rates.

1. Program-wide Claims Analysis/Health Claims Data Warehouse

The challenge for OPM is that, while the FEHBP directly bears the cost of health 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. 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. The data will be derived from health and prescription drug claims under the FEHBP. The HCDW will allow OPM to understand the drivers of cost increases and model the potential effects of health system reform or environmental changes on Federal employees. This warehouse will also strengthen OPM's ability to strategically shape future benefits design by better positioning the agency to negotiate effectively with the FEHBP carriers to keep premium increases below industry-wide levels.

During FY 2010, OPM began the processes necessary to implement this searchable and secure database for claims information, which included:

- To build analysis capacity and infrastructure, OPM hired a project manager and a health economist. These new additions have begun work with existing data analysis and policy staff on the creation of the HCDW.

- The HCDW team has created a risk management plan which establishes the processes and procedures for dealing with risks associated with the HCDW. It focuses on the processes and procedures the team will follow to identify, categorize, manage, document, track, and close risks throughout the project lifecycle.

- The HCDW team has also selected and hired a project management organization (PMO). The PMO is now working to create a comprehensive project management plan to ensure the effective design, implementation, maintenance and data analysis of necessary health claims data.

- Currently, the HCDW team is compiling intended data use needs for the HCDW requirements document. A thorough completion of this step will ensure that the completed warehouse will have the capability to allow analysts to effectively analyze costs and provide adequate management support for the Program.

It is important to note that developing and maintaining a health claims data warehouse of this magnitude presents its own complex challenges [including managing multiple data formats and feeds; large size; security; data validation and verification; flexibility (health care is a dynamic industry); etc.].

2. Prescription Drug Benefits and Costs

Increases in drug costs have been a major contributor to the rapid growth in health care costs over the last few years, with drugs now accounting for about 29 percent of all FEHBP costs. Of particular concern to our office are the pharmacy benefit managers (PBMs), who administer drug benefits for the FEHBP carriers. The FEHBP carriers, not OPM, negotiate the pricing of these pharmacy benefits. Currently these contracts lack transparency, which limits our ability to audit and provide adequate oversight of this high cost benefit. This lack of transparency makes it impossible for OPM to ensure that FEHBP enrollees are receiving quality benefits at a fair price.

There also continues to be Congressional interest in the lack of transparency and high cost of prescription drugs within the FEHBP. During this fiscal year, our office participated in a Congressional hearing for the purpose of providing comments to a proposed bill (H.R. 4489 - "FEHBP Prescription Drug Integrity, Transparency, and Cost Savings Act"). This bill was drafted to address the many concerns raised over the FEHBP's prescription drug program. Until such time that

these concerns are addressed, either by the passage of the bill or through actions undertaken by the Agency, we anticipate Congressional interest in this area to continue.

For its part, OPM's PBM working group, established to consider short and long-term initiatives to strengthen the controls and oversight of the FEHBP pharmacy benefits, accomplished the following during this fiscal year:

- Issued Carrier Letter #2010-04, "Pharmacy Benefits Management (PBM)," to the fee-for-service carriers participating in the FEHBP. The purpose of the letter was to outline new transparency principles, which are to be included in future PBM procurements beginning in contract year 2011 and going forward. Specifically, the principles required the following:
  - Pass-through transparent pricing in carrier contracts with PBMs;
  - PBM's profit under the contract must be tied to clearly identifiable sources;
  - PBM's administrative fees must be clearly identified to retail claims, mail claims, and clinical programs, if applicable; and,
  - Contracts and other documentation supporting charges to the carrier must be fully disclosed to and auditable by the carrier or its agent and the OPM Office of the Inspector General (OIG).
- Proposed amendments to the contract language for OPM's fee-for-service carriers and experience-rated HMOs, requiring them to ensure that their new, renewing, or amended PBM contracts, effective January 2011 going forward, include certain transparency standards.
- Contracted with an outside vendor to explore alternative approaches/changes in contracting arrangements with PBMs, such as:
  - Using the Federal Supply Schedule to purchase prescription drugs at a lower cost;
  - Carving out pharmacy services from the existing FEHBP benefit structure; and,
  - Developing an alternative prescription drug plan design.

Due to the complexities and the significant costs associated with the FEHBP pharmacy benefit program, it is critical that all alternative approaches be carefully evaluated and modeled before implementing changes. Changes must ensure the health and safety of all FEHBP enrollees and be cost effective.

3. Radiology and Imaging

Radiology costs in the United States have grown to more than $100 billion annually. Diagnostic imaging is the second-largest and fastest-growing expense for health plans (behind pharmaceuticals). Factors driving this growth include the fragmentation of care, continual advances in diagnostic imaging technology, the affordability of imaging equipment leading to adoption and utilization in more care settings, direct advertising to patients, and an aging population.

OPM has not yet developed the program-wide data base for analyzing use rates, trends, and patterns or excess. However, they have communicated to carriers the undesirability of the overuse of imaging technology through value negotiation and other outreach. Strategies that they have encouraged carriers to adopt include:

- reducing benefit costs by avoiding unnecessary utilization;
- increasing patient safety by reducing exposure to radiation;
- educating providers on the appropriate procedure for specific medical conditions using evidence-based radiology criteria;
- encouraging pre-approval for use of imaging services;
- assuring (through "credentialing") that equipment is safe and not outdated; and,
- assuring that radiologists and support staff are adequately trained and available.

OPM has also encouraged management of radiology and imaging benefits by providing carrier education. At the annual FEHBP Carrier Conference, MedSolutions, an industry imaging consultant and support services provider, spoke on balancing effective treatment with cost. Some carriers (e.g., CIGNA and the Government Employees Health Association) employ MedSolutions or similar organizations to review and approve claims prior to treatment, or to suggest alternative diagnostic choices.

B. National Healthcare Operations

1. Patient Protection and Affordable Care Act

Under the Patient Protection and Affordable Care Act (PPACA), OPM has been designated as the agency responsible for implementing and overseeing the multi-state plan options. In accordance with the PPACA, at least two multi-state plans will be offered on each state health insurance exchange beginning in 2014. Multi-state plans will be one of several health insurance options that small employers and uninsured individuals will be able to choose from. In total, state exchanges are expected to provide health insurance coverage for as many as 31 million Americans. In addition, the PPACA incorporated the Indian Health Care Improvement Reauthorization and Extension Act of 2009. This Act allows certain Indian tribes, tribal organizations, and urban Indian organizations to purchase FEHBP coverage.

While implementing any new program represents a host of complex challenges, one of the greatest challenges will be securing sufficient resources for OPM's new national healthcare function, as well as the expanded FEHBP-eligible population. Currently, the PPACA does not specifically fund OPM for its new healthcare responsibilities. In addition, it requires that essential resources not be pulled away from FEHBP in order to start up the new programs. Thus, OPM has discussed FY 2011 and FY 2012 funding requirements with both the Department of Health and Human Services (HHS) and the Office of Management and Budget. Funding beyond FY 2012 is also a significant challenge for the agency, as well as for the

OIG, who is charged with program oversight responsibilities. Without additional resources, OPM will not be able to support these new activities.

2. Pre-Existing Condition Insurance Plan

As part of PPACA, HHS was required to develop and implement a Pre-Existing Condition Insurance Plan (PCIP) within 120 days of enactment of the Act. This program makes health insurance available to those who have been denied coverage by private insurance companies because of a pre-existing condition, have been uninsured for at least six months, and are U.S. citizens or are residing in the U.S. legally.

Due to OPM's experience in administering the FEHBP, HHS turned to OPM for assistance. By employing an *advances and reimbursements agreement* with HHS, OPM was able to design and implement the PCIP as required by PPACA. While the implementation was successful, administering this newly created program represents an ongoing management challenge for OPM.

3. BACKGROUND INVESTIGATIONS

OPM's Federal Investigative Services (FIS), headquartered in Boyers, Pennsylvania, conducts background investigations on Federal applicants, employees, military members, and contractor personnel for suitability and security purposes. FIS conducts approximately 90 percent of all personnel background investigations for the Federal Government and processes approximately 2 million investigations per year.

Twelve background investigators have been criminally convicted since 2007. Ten were convicted of fabricating background investigation reports, to include reporting interviews that never occurred, recording answers to questions that were never asked, and documenting record checks that were never conducted. The remaining two background investigators were convicted of other forms of misconduct.

FIS has a system of internal controls in place to detect fraud and is to be complimented on their efforts in recent years to aggressively pursue wrongdoing on the part of Federal and/or contractor staff, on their referral of suspected fraud to the OIG, and on their efforts to work jointly with the OIG to bring offenders to justice. Nevertheless, this is a long-term problem that requires continued close attention by OPM management.

Agencies use the reports of investigations conducted by OPM to determine individuals' suitability for Federal civilian, military, and Federal contract employment, as well as their eligibility for access to national security classified information. If a background investigation contains incorrect, incomplete, or fraudulent information, a qualified candidate may be wrongfully denied employment or an unsuitable person may be cleared and allowed access to Federal facilities or classified information. Therefore, any fraud in background investigation reports has serious national security implications.

While the integrity assurance internal controls utilized by FIS are very effective, they can only detect fraud after it has already occurred. Therefore, an emphasis on prevention and deterrence is critical. We note and applaud FIS's commitment to providing integrity awareness training to its staff. We also observe that criminal prosecution is an effective deterrent to fraud. However, in any employee and/or contractor population, a small percentage will always be inclined towards fraud/dishonesty, no matter how much training they are provided or how much effort is put into hiring trustworthy people. While FIS can and does attempt to mitigate this risk, they cannot remove the risk entirely. Therefore, it is vital that both FIS and the OIG continue to work together to continuously evaluate its internal control structure and pursue criminal prosecution of background investigators who engage in falsification of work product. The OIG has performed audit work in addition to the investigative work referred to above, although this work is limited due to funding limitations of the OIG to perform the Revolving Fund work, which the OIG this year has identified as a material weakness within its own office.

INTERNAL CHALLENGES

The following challenges relate to current program activities that are critical to OPM's core mission, and that while impacted to some extent by outside stakeholders, guidance, or requirements, they for the most part are OPM challenges that have minimal external influence. They are areas that once fully implemented 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 SYSTEM DEVELOPMENT

In two reports to Congress (GAO-06-184 and GAO-09-529), the Government Accountability Office (GAO) described significant shortcomings in OPM's ability to successfully manage large and complex information systems development projects. These shortcomings were primarily attributed to a lack of disciplined processes in several key areas, including investment management, requirements management, testing, project oversight, risk management, and information security.

OPM has a long history of failed system development projects, and systems that were delivered with less functionality than desired. In 1987 OPM began a series of projects aimed at automating and modernizing the business process of handling retirement applications from federal employees. Initially known as the Federal Employee Retirement System Automated Processing System and currently known as the RSM project, the efforts to modernize OPM's retirement systems have spanned 19 years producing limited results.

Another system that has not delivered the intended functionality is the agency's new financial management system, known as CBIS. This system was scheduled for implementation in two phases involving several releases. The first release was put in place

on October 1, 2009; since then there have been numerous problems involving system functionality and business process conflicts.

Finally, the Service Credit Redeposit and Deposit System (SCRD) was taken offline after implementation because it could not meet the basic requirements of the business process. This occurred because of a lack of disciplined processes in requirements management and change management. As a result, customers have experienced significant inconvenience; OPM staff has been forced to introduce manual workarounds which are taxing limited resources; and the agency faces potentially major political scrutiny, not to mention potential legal problems.

Implementing disciplined processes in the functional system development areas will be a major internal management challenge for the agency as it takes on these and other IT system projects.

A. Retirement Systems Modernization

Processing the retirement payments of Federal employees is a mission-critical OPM program. As the administrator of the Federal employees' retirement program, OPM is challenged with the massive scale and complexity of supporting over 2.9 million active employees, 2.5 million annuitants, and managing the Federal retirement and disability trust fund, which consists of over $790 billion in assets.

The RSM program is OPM's long-term initiative targeted at implementing modern technology and tools to help improve the efficiency and effectiveness of OPM's Retirement Program. RSM is critical for two reasons: 1) the workload of the Retirement Program staff has grown over the years and will continue to grow as up to 60 percent of the Federal workforce will become eligible to retire in the next 10 years; and 2) the Retirement Program's aging systems and paper-based processes cannot fully support the needs of the program and expectations of their customers – providing timely and accurate benefit payments to more than 2.5 million annuitants and their families.

While OPM depends on aging IT systems to estimate benefits and to pay its retirees, the RSM program has faced a number of challenges modernizing the system(s) over the years. Consistent with the findings of GAO in 2009, OPM identified and focused on delivering the key "building blocks" (functions) needed to automate the retirement process. Delivering modern, improved retirement services, including a web-enabled retirement application, self-service tools, retirement estimators, and a comprehensive retirement case management system, is dependent on putting the core "building blocks" in place first. Those core "building blocks" include:

- Prioritizing fixes to retirement calculators and supporting systems based on need and age;
- Building a data warehouse capable of receiving electronic retirement data and imaged records from Federal agencies and shared service centers; and,

- Implementing retirement data feeds with agencies and shared service centers so that a single standard set of information could be exchanged across the government.

The RSM program is now challenged with determining the best solution for delivering much-needed improvements to OPM's retirement calculation systems, starting with the Federal Annuity Calculator and Estimator System, which aids retirement specialists in processing the majority of retirement claims. Improvements to the retirement systems are dependent on continued funding in order to deliver the following:

- Documentation and validation of business rules to enable any future solution to correctly calculate annuities of retiring Federal employees;
- Retirement data feeds that ensure data received is accurate, complete, useable, and compatible with the technology solution;
- Technology solutions and other systems involved in RSM that are secure in accordance with FISMA and comply with all relevant laws, regulations, rules and official guidance that govern the design and creation of electronic systems of record; and,
- Users are properly and adequately trained to use the technology solution in order to provide effective and efficient customer service.

During this transition period, OPM must continue to maintain the existing legacy processes and process claims for annuitants and survivors with limited technology, and increased workloads and customer service expectations.

RSM made great progress in FY 2010 with respect to documenting the Federal laws, rules and calculations necessary to process all Federal retirements; building the data warehouse capable of receiving electronic retirement data; and defining the Federal government standard by which retirement-related data will be sent to OPM by shared service centers and agencies.

The need to pay Federal annuitants in a timely and accurate manner is as critical as ever to OPM's mission. The RSM program must continue to build upon the progress made in FY 2010 and meet these challenges to continue moving forward in providing a technology solution to modernize the Federal retirement systems.

B. Consolidated Business Information System

CBIS is OPM's new financial management system. Phase 1 Release 1 of the system, which involved OPM's Revolving Fund and Salaries and Expenses accounts, was implemented in October 2009.

Almost immediately it was clear that there were significant problems with this new system as customers encountered issues with access, workflow, and information gaps. There were also technical problems that impacted invoice payments, travel vouchers, and financial reporting.

In March 2010, OPM formed a Tiger Team to perform a complete review of the CBIS program and recommend appropriate corrective action. The Tiger Team created an overall CBIS improvement plan that focused on eight critical project areas. The plan also recommended a leadership timeout to reflect on project successes and remaining challenges; and a Lean Six Sigma review to improve quality by minimizing defects and variability in financial-related business processes.

The Tiger Team also recommended delaying the implementation of Release 2, which was originally scheduled for April 1. This release was eventually implemented on August 21, 2010, and included functionality enhancements and corrections for some of the Release 1 issues.

Going forward and preparing for the implementation of Phase 2, which includes the Trust Fund accounting, OPM will face significant challenges as it continues to work through the action items identified in the CBIS improvement plan. By applying disciplined processes and best practices in IT project management, the technical and managerial issues will likely be resolved; however, a more daunting challenge may well be adapting the existing business processes and organizational culture to the standard business processes and rules of core federal financial management functions.

C. Service Credit

Under the Civil Service Retirement System (CSRS), employees may make optional deposits for periods of service during which retirement contributions were not withheld from their pay. They may also redeposit refunds of retirement contributions during previous periods of service. Employees who are covered by the Federal Employees Retirement System (FERS) may make optional deposits of retirement contributions that were not withheld from their pay, but, prior to October 28, 2009, they could not redeposit refunds of retirement contributions. Under either system, interest is due on the deposited or re-deposited amounts, although interest rates and periods vary. The purpose of making these deposits or re-deposits is to obtain credit toward retirement for previous periods of service.

Until 2006, this process was facilitated by a mainframe-based information system that had been in place for many years. This system handled basic transactions, including initial billing and interest calculations, but it was not designed to accommodate the many complexities of the business process, particularly the special retirement rules for various classes of Federal employees. These more complex transactions were processed manually.

In April 2006, OPM released a new version of the service credit system which was designed to allow most types of transactions to be automatically processed on users' desktop computers. In early 2008, users identified anomalies in payment and interest amounts, and it was eventually discovered that the system was not properly calculating interest in some cases.

Initial attempts to correct the problems were not successful, and the system was eventually taken offline in July 2008. Some fixes were later applied and the system was brought back on-line for limited use in October 2008; however, resource intensive manual workarounds continue to be necessary and account holders have not received updated statements.

For over two years, OPM has been working to identify all existing problems in the SCRD application, apply corrective action, and implement an updated system that properly handles the majority of service credit cases. The OIG reviewed the initial system development process to determine the cause of the system failure, and the ongoing efforts to redeploy the system.

Overall we discovered a serious lack of disciplined processes involved in the initial system development project and the early efforts to correct and redeploy the system. There were weaknesses throughout the system development lifecycle, but especially in project management, requirements management, and change management.

OPM recently applied improved processes to the current remediation effort, including a more systematic project management process, better change management and separation of duties, improved development, and a more rigorous testing process. However, major challenges remain. In the near term, OPM management must develop a plan that provides resolution to account holders who have been affected by the system problems. In addition, there is likely to be intense political scrutiny. Management must be prepared to present an effective communications and congressional liaison strategy, including possible legislative relief for affected account holders.

In the long term, OPM will probably need to scrap the existing system and develop a new system that adheres to standard best practices of a payment and billing system. This may also involve some business process reengineering. It will be critical to ensure that disciplined processes are followed throughout the system development lifecycle.

2. INFORMATION SECURITY GOVERNANCE

OPM relies on information technology to manage its core business operations and deliver products and services to many stakeholders. With increasing reliance on information systems, growing complexity, and constantly evolving risks and threats, information security has become 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 needed 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 several years, the OIG has reported increasing concerns about the state of the agency's information security governance. In May 2009, the OIG issued a Flash Audit Alert (FAA) to the OPM Director and the Chief Information Officer (CIO) highlighting these concerns. The primary issues outlined in the FAA included outdated information security policies and procedures, and an understaffed IT security program, particularly the longstanding lack of a permanent senior agency information security official (SAISO).

Our FY 2010 Federal Information Security Management Act (FISMA) audit indicated that very little progress has been made in correcting these issues. The underlying cause, in our opinion, is that OPM has not established adequate information security governance activities in accordance with legislative and regulatory requirements. Specifically, the agency has not fully documented information security policy and procedures or established appropriate roles and responsibilities.

The lack of policies and procedures was reported as a material weakness in the FY 2007 and FY 2008 FISMA audit reports. In FY 2009, we expanded the material weakness to include the agency's overall information security governance program and incorporated our concerns about the agency's information security management structure. This material weakness continued in FY 2010, even though the agency finally appointed a new SAISO, because of ongoing concerns about the lack of resources devoted to the IT Security and Privacy Group within the Office of the Chief Information Officer (OCIO).

We have learned that the OCIO has secured approval for additional staff in this group, including contractor support. The OCIO also has an Interagency Agreement with the Department of Treasury's Bureau of Public Debt to assist with policy development. We will evaluate progress in these areas in FY 2011.

We reported a second material weakness this year related to OPM's information system certification and accreditation (C&A) process because of longstanding flaws and deteriorating conditions. In FY 2008 and FY 2009, we reported that weaknesses in the C&A process were a significant deficiency in the internal control structure of the agency's IT security program. The weaknesses cited related to inadequate management of the process and incomplete, inconsistent, and poor quality C&A products. In FY 2010, these longstanding conditions not only continued, but actually worsened. As a result, we reported a material weaknesses in the IT security control structure related to OPM's C&A process.

We believe that the root cause of these issues is related to poor information security governance, as described above, but also to the OCIO's perspective of its role in IT security at the agency. An IT security program can be structured with a centralized or decentralized model, although most agencies adopt a hybrid structure with characteristics of both approaches. OPM, however, has chosen to implement a highly decentralized structure with

most of the responsibility for IT security in the program offices, with the OCIO responsible for policy development and oversight.

While it is true that IT security should be a shared responsibility between the OCIO and the program offices, FISMA assigns ultimate responsibility to the CIO for developing and maintaining an effective IT security program. Our audits over an extended period of time have clearly shown that OPM's decentralized approach is not effective. Program offices, in general, have neither the expertise nor the interest in properly managing an IT security program for their systems. Program offices will naturally focus limited resources on operational issues, and IT security is normally a secondary concern.

In our FY 2010 FISMA report we recommended that OPM adopt a more centralized approach to IT security. We suggested that the agency recruit a staff of information security professionals to act as designated security officers (DSO) that report to the SAISO. This model would replace the existing approach where current DSOs, most of whom have no background in IT security, report to their program offices. The OCIO has agreed with our recommendations for a more centralized IT security structure. However, implementing this new strategy will most likely be complicated by budget issues, concern about access to systems, and opposition to change.

Clearly management faces a major challenge in correcting the ongoing and very serious deficiencies in information security governance at OPM.

3. FINANCIAL MANAGEMENT SYSTEM AND INTERNAL CONTROLS: REVOLVING FUND AND SALARIES AND EXPENSES ACCOUNTS

During the current audit of OPM's FY 2010 financial statements, the auditors noted that deficiencies continue to exist in the operation of the Office of the Chief Financial Officer's internal controls over financial management and reporting, affecting the accuracy of the Revolving Fund (RF) and Salaries and Expenses Accounts (S&E). These deficiencies are attributed to:

1. CBIS does not properly process and display all appropriate financial information in accordance with Federal Financial Management Improvement Act requirements and is not properly configured to produce useful financial reports that provide accurate information regarding related intra-governmental activities and balances;
2. OPM has not completely identified existing differences between its own internal data and the information reported by the U.S. Department of the Treasury (Treasury) resulting in an imbedded difference in its Fund Balance with Treasury (FBWT) amount; and,
3. OPM has not effectively enforced procedures related to the consistent and clear documentation of the performance of Salaries & Expenses Fund reconciliations and as outlined in the "Treasury Financial Manual" and OPM's "Cash Management Policy and Procedures."

OPM has had a long standing issue with reconciling its RF account with Treasury. Revisions to the work instructions for reconciling the cash balances to the FBWT for the

RF were made in FY 2009 to include strict deadlines for the completion of monthly reconciliations. With the implementation of the new financial system, CBIS, management still continues to have internal control weaknesses with FBWT reconciliations for the S&E and RF. OPM is challenged to continue to improve business processes within CBIS to address the current deficiencies.