Office of the Inspector General
United States Office of Personnel Management

Statement of the Honorable
Patrick E. McFarland
Inspector General
U.S. Office of Personnel Management

before the

House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Federal Workforce, U.S. Postal Service
and Labor Policy

on

"Back to the Basics: Is OPM Meeting its Mission?"

November 15, 2011

Chairman Ross, Ranking Member Lynch, and Members of the Subcommittee:

Good morning. My name is Patrick E. McFarland. I am the Inspector General of the U.S. Office of Personnel Management (OPM). Thank you for inviting me to testify at today's hearing about OPM's use of information technology (IT) to fulfill its core missions. As the Federal Government's human resource office, OPM plays a critical role in recruiting, retaining, and providing employment-related benefits to a world-class workforce that serves the American people.

Today's hearing focuses on the role of IT systems in fulfilling the first and last of these responsibilities: OPM's role in the hiring and retiring phases of a Federal

employee's career. I urge the Subcommittee to look at these issues in the broader context of how OPM implements and utilizes IT policies and systems on an agency-wide basis.

IT Systems Development

OPM relies upon IT systems to manage its core business operations and deliver products and services to many stakeholders. As others here will discuss in more detail, OPM has long struggled with modernizing its retirement IT system and, more recently, has encountered problems with the launch of USAJOBS 3.0. An April 2009 Government Accountability Office report (GAO-09-529) concluded that OPM's past shortcomings in systems development can primarily be attributed to a lack of disciplined processes in several key areas, including investment management, requirements management, testing, project oversight, risk management, and information security.

We believe that a key cause of OPM's challenges in this area can be traced to the lack of institutional knowledge within OPM concerning system development life cycle (SDLC) processes. SDLC is a process for building information systems in a very deliberate, structured, and methodical way. We believe that an important first step is for OPM to start building this institutional knowledge by retaining one or more individuals within its Office of the Chief Information Officer (OCIO) who understand SDLC processes and have successfully used proven methodologies for large scale system development projects.

Once OPM has that institutional knowledge, it could properly evaluate its current SDLC processes; make appropriate revisions; and communicate the requirements to all agency program offices. This SDLC expertise would be used to oversee all OPM system development projects and as a resource for project managers.

I cannot stress how important it is to have the correct processes in place at the beginning of any project. It is much easier (and more efficient) to invest the time and resources necessary to develop the right procedures to use going forward than it is to go back and fix problems after they occur.

USAJOBS 3.0

I know that the Subcommittee is particularly interested in the recent implementation of USAJOBS 3.0. We too have concerns. However, we have not had an opportunity to review the USAJOBS 3.0 system development process. Therefore, we plan to initiate two audits of USAJOBS 3.0 this fiscal year. We are

already in the planning phase for the first audit, which will cover IT security. Our objectives will be to verify that appropriate IT security controls are in place to minimize the risk of security breaches similar to those that occurred with the prior contractor.

The second audit will be to determine if OPM followed a disciplined systems development process focusing on investment management, requirements management, testing, project oversight, and risk management.

IT Security Governance

The other vital issue related to the management of diverse and complex IT systems such as those overseen by OPM is properly managing an information security program to reduce risk to agency operations.

Information security governance is the overall framework and supporting management structure and processes that are the foundation of a successful information security program. Proper governance requires that agency management proactively implements the cost-effective controls needed to protect the critical information systems that support the core mission, while also managing the changing risk environment. In this context, "governance" refers to 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 have expressed concerns in audit reports about OPM's IT security program. Specifically, the agency had outdated information security policies and procedures, an understaffed IT security program, and (for almost two years) no senior agency IT security official (SAISO). Under the leadership of the current Chief Information Officer, OPM made progress in addressing these concerns during fiscal year (FY) 2011. It updated most of its security policies and procedures, increased the IT security staff, and retained a permanent SAISO.

There is still, however, the problem that OPM's IT security program is highly decentralized, meaning that the OCIO and OPM's program offices share responsibility for IT security. In practice, this has meant that most of the management of IT security is in the program offices, with the CIO providing policy development and oversight. We do not believe that this division of responsibility is satisfactory because OPM program offices tend to focus their resources and efforts on operational issues and make IT security a secondary concern. Consequently, we continue to recommend that the OCIO be given the

resources necessary to centralize the responsibility for the security of OPM IT systems.

Non-IT Concerns

It is important to point out that IT programs are neither the source of nor the solution to all of OPM's problems related to its core functions.

I am particularly troubled by OPM's continuing pattern of making improper payments to deceased annuitants, necessitating the expenditure of significant resources to recover these monies. Resources should instead be used to identify and, more importantly, prevent improper payments from being made. We have been working closely with OPM on this issue for over six years, and while improvements have certainly been achieved, systemic problems remain.

My office's efforts began in 2005 when we initiated a study of best practices for preventing improper payments to deceased annuitants. Along with OPM representatives, we met with several benefit-paying Federal agencies and a major corporation to discuss procedures and internal controls that were used to prevent and detect improper payments. This study resulted in a report that we provided to the OPM Director containing recommendations for improvements related to preventing improper payments from the Federal Government's Civil Service Retirement and Disability (CSRD) Fund. We updated and reissued this report in January 2008, reflecting the progress that the agency had made in addressing our original recommendations, and providing additional recommendations. While a number of improvements have been implemented since then, it has become clear that they were only partial remedies. Consequently, my office issued a third report in September 2011 to again highlight the need for aggressive action in this area.

This report, "*Stopping Improper Payments to Deceased Annuitants,*" attempted to demonstrate the need to stop the flow of improper payments once and for all from the CSRD Fund to deceased annuitants, which have averaged $120 million annually over the last five years. It is important to note that this entire amount does not represent long-term improper payments. Much of it - although OPM could not provide the exact amount - comes from improper payments that are identified and recovered in a matter of a few months. These are often the result of a retiree passing away just before the retirement payment is made for that month, or because the deceased's family takes a month or two to report the death. These payments are usually recovered in full.

While of course we would like to prevent all post-death improper payments, as each one requires time and effort to recover, our paramount concern is with those payments resulting when an annuitant's death is not properly reported or detected and which then continue for many years. These payments are frequently taken by a relative or guardian of the deceased annuitant who neglected to report the death. In many cases, these individuals then actively lead OPM to believe that the annuitant was still alive by forging his or her signature on an inquiry form from the agency. Our experience is that these improper payments often cannot be recovered.

As an example, our report noted the case of an annuitant's son who continued to receive benefits until 2008, 37 years after his father's death in 1971. The improper payment in this case exceeded $515,000 and was reported to OPM only when the son died. None of these funds could be recovered. While this is a larger than average improper payment, it is not unusual for these amounts to exceed $100,000. Despite the improvements that have been implemented, there remains a high probability that this egregious loss of monies from the CSRD Fund will continue. Each year we identify new cases which support this concern.

Based upon our recommendations, OPM has taken positive steps to address this issue. Regular meetings over the last three years between OPM subject matter experts and my office have led to enhanced identification and prevention measures. These measures need to be further refined, incorporated into routine business processes, and monitored on a continuous basis by senior management.

Currently the key initiatives include:

- **Computer matching**: OPM will conduct an annual computer match between the OPM retirement annuity roll and the Social Security Death Master File to identify deceased annuitants who continue to receive annuity payments. The agency has just begun performing the match for this year.

- **Increasing contact**: The retirement program office will systematically contact a sample of the annuity roll population over 90 years old and request that they send OPM a signed response confirming their vital status and validating their correspondence address. It has conducted this exercise once and plans to do so every other year going forward, with the next effort scheduled for later this fiscal year.

- **Analysis of undeliverable correspondence**: Under Treasury regulations, OPM must annually send annuitants an IRS Form 1099-R reporting the amount of the annuity that the retiree received during the calendar year. OPM has agreed to analyze undeliverable correspondence, focusing on these Forms 1099-R, and contact those annuitants to determine why the mail was returned. OPM is currently in the process of performing this project for the Forms 1099-R returned in January 2010.

- **Recovering improper payments from financial institutions**: OPM is attempting to improve and streamline the process whereby it works with U.S. Department of the Treasury to reclaim improper payments to deceased annuitants directly from the back accounts where they were electronically deposited.

In addition, we have strongly recommended that OPM establish a permanent working group of retirement program subject matter experts to focus on improving the retirement program's integrity. This group would identify and explore risk areas and take advantage of the wealth of information contained in the annuity roll by, for example, developing data mining programs that would search for anomalies indicating possible improper payments or fraud.

Conclusion

OPM operates a wide range of complex, governmentwide programs. The agency has been largely successful in providing the Federal Government with the human resources support that it requires. However, OPM also must continue to evolve and adapt to an increasingly automated world. To do this, it needs both the leadership and the resources to properly plan and carry out such initiatives. To this end, we have been working closely with Director Berry to see that OPM meets the challenges ahead of it. We particularly appreciate Director Berry's proactive support.

Thank you again for inviting me here today. I would be happy to respond to any questions you may have.