REMARKS OF BRIAN MILLER
INSPECTOR GENERAL
GENERAL SERVICES ADMINISTRATION

BEFORE THE
FEDERAL CHIEF INFORMATION OFFICERS COUNCIL

IMPROVING INFORMATION TECHNOLOGY INVESTMENT MANAGEMENT PRACTICES IN THE FEDERAL GOVERNMENT TO BETTER PREVENT AND DETECT FRAUD, WASTE, AND ABUSE WITH IMPLEMENTATION OF THE RECOVERY ACT

Friday, August 7, 2009

Good morning. My name is Brian Miller and I am the Inspector General (IG) at the General Services Administration (GSA). Thank you for providing me the opportunity to speak to you today about Inspectors General (IGs) views on improving information technology (IT) investment management practices and results in the Federal government to better prevent and detect fraud, waste, and abuse with implementation of the American Recovery and Reinvestment Act (Recovery Act). The IT dashboard initiative is an important step in providing transparency, accountability, and visibility into the Federal government's IT portfolio. As you know, through this initiative, Federal agencies and the public will have the ability to view details of Federal IT investments online and to track their progress over time. A collaborative approach involving IGs, Chief Information Officers (CIOs), and other stakeholders can lead to successful implementation of this initiative and enhance IT risk management practices government-wide. Working together also is important to ensure that Federal IT systems are supporting implementation of the Recovery Act and providing management information to assist in the prevention and detection of fraud, waste, and abuse.

The need for IGs and CIOs to work collaboratively to address the challenges associated with managing information technology has, perhaps, never been greater. The President's FY 2009 enacted budget provides for approximately $75 billion for information technology investments across the government.[1] Further, the Recovery Act includes $787 billion to create jobs and stimulate the economy through a variety of measures that modernize the Nation's infrastructure and improve energy independence.[2] The Recovery Act impacts IT management in the government, since existing IT systems may need to be changed to support new reporting requirements and new system connections – both internal and external to agencies – may need to be established. Recovery Act funds may also be used to develop new information systems. Moreover, we must utilize information system controls to assist us in preventing and detecting fraud, waste, and abuse with Recovery Act implementation.

[1] http://it.usaspending.gov/?q=content/current-year-fy2009-enacted

[2] American Recovery and Reinvestment Act of 2009, Public Law 111-5, February 17, 2009.

Under the Inspector General Act of 1978, the Office of Inspector General is required to, among other things, (1) conduct independent and objective audits, investigations, and inspections; (2) prevent and detect fraud, waste, and abuse; and (3) promote the economy and efficiency of agency programs. With implementation of the Recovery Act, these responsibilities are even more important, as funds will be spent with increased speed and volume. As CIOs, you have an unique understanding of the challenges associated with ensuring that our IT systems support Recovery Act activities and implementing the technological initiatives needed to streamline government operations and increase transparency.

At GSA, my office works closely with Casey Coleman, the GSA Chief Information Officer, and other senior IT decision makers to plan and conduct IT audits that seek to address challenges that GSA faces with strategically managing IT to meet agency goals. Audits performed by my office include coverage of: GSA's information technology security program, as required by the Federal Information Security Management Act (FISMA), system development efforts in GSA, privacy controls, and capital planning and investment control processes. In her role as Chief Information Officer at GSA, Casey's vision and leadership have led to several positive changes to IT management at GSA. For example, GSA has been implementing blogs and other collaboration tools to increase citizen participation in government and improve internal agency communications. As part of this effort, GSA has developed a policy for "social media" technologies, such as blogs. As you may know, Casey is also leading efforts to evaluate "cloud computing" technologies for government-wide use (more to say on this later).

Today, I would like to discuss three main areas: (1) ensuring that accurate and reliable data on IT investments are collected, maintained, and reported; (2) ensuring adequate governance of IT systems; and (3) key IT risk management challenges from an Inspector General viewpoint. Working together, we can strengthen risk management processes for providing transparency and accountability in the government's IT portfolio. Likewise, I believe that making improvements in these areas also will better enable us to leverage IT systems to best support implementation of the Recovery Act as well as to detect fraud, waste, and abuse.

(1) Ensuring that Accurate and Reliable Data on IT Investments are Collected, Maintained, and Reported

As CIOs, you play a key role in meeting legislative requirements related to the management of information technology. Further, you work under a governance framework that is required within the Executive Branch for managing IT. Studies and reports of CIO responsibilities in the private and public sector have noted that an effective CIO can make a significant difference in building the institutional capacity needed to improve an agency's ability to manage information and technology, and thus enhance program performance.[3] However, CIOs may not always have the operative means of ensuring the delivery of IT mission and business programs—in other words they may be "empowered but not enabled." You are "empowered" by the law, but you may not control operational spending and sometimes, not even the operations themselves. This provides an opportunity for IGs and CIOs to work together to convince agencies to correct deficiencies and strengthen risk management processes.

[3] See for example GAO-06-201T, "The Role of the Chief Information Officer in Effectively Managing Information Technology."

One key to effectively assessing, managing, and evaluating the risks associated with IT investments is to ensure that accurate and reliable performance, cost, and schedule data is collected, maintained, and reported. This also is important for independent verification of reported IT investment goals and performance measures. As you know, the Office of Management and Budget (OMB) requires agencies to identify estimates for all IT investments using an Exhibit 53. Further, for "major IT investments," agencies must develop capital asset plans and business cases, known as the Exhibit 300. Information included in these exhibits includes performance measures, milestones, cost and schedule data, and information on security and privacy. Currently, these exhibits serve as the primary input to the IT dashboard initiative.

In January 2007, in response to questions raised by the Government Accountability Office (GAO) regarding the reliability of agency IT budget submissions, the OMB Administrator for Electronic Government and Information Technology expressed interest in having the Inspector General community ascertain the validity of information contained in the exhibits. In response, the Chair of the Audit Committee of the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency asked IGs to identify those assessments conducted during FY 2006 or later that provide insightful information about the reliability of agency budget submissions. A summary of the report can be found at http://www.ignet.gov/pande/audit/omb300.pdf. While the information contained in this document is based on work performed by OIGs in FY 2006 and FY 2007, the issues identified remain pertinent as we consider how best to utilize the IT dashboard initiative. Moreover, this summary report highlights a significant body of work performed by IGs across the government related to the accuracy and reliability of IT budget submissions.

Ensuring the accuracy and reliability of data generated and maintained by IT systems also is a concern for IGs as we respond to our oversight responsibilities under the Recovery Act. Last summer, my office established a forensic audit unit that uses advanced computer investigative work – such as data mining and analysis – to discover fraud. Successful forensic auditing techniques oftentimes utilize data in IT systems to discover and prevent fraud. Including additional information on the IT dashboard, such as relevant IG reports, US-Computer Emergency Readiness Team statistics, and system privacy impact assessments may provide a more comprehensive view of IT systems and also increase transparency and accountability.

(2) Ensuring Adequate Governance of IT Systems

Accurate and reliable data on IT systems are also needed to support an IT Governance structure that aligns IT investments to strategic goals, which is my second topic of discussion. The Information Systems Audit and Control Association has defined IT governance as consisting of the leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives. In other words, IT governance supports business goals, optimizes IT investment, and appropriately manages IT-related risks and opportunities through an internal control framework.

Unfortunately, news media are filled with stories of weak IT governance processes that have contributed to Federal government projects being delivered over budget and cost, while not meeting user needs. For example, last year *The Washington Post* reported that government

auditors found 95 major weapons systems at the Department of Defense that exceeded their original budgets by a total of $295 billion, bringing their total costs to $1.6 trillion. Auditors also found that, on average, these projects were delivered almost two years late.[4] Similar incidents that highlight weaknesses in IT governance processes have been reported at other agencies. For example, in 2006, the Department of Veteran Affairs (VA) disclosed that a computer laptop and external hard drive containing sensitive data on millions of veterans were stolen from the home of a VA employee. This loss of data by the VA was a risk that IT governance failed to identify and mitigate.

IGs and CIOs can work together to evaluate and enhance IT governance processes so that taxpayer interests can be protected and any problems with systems development, operation, and maintenance flagged so that prompt action can be taken. I would like to highlight two areas in particular where IT governance processes can be improved to better protect tax payer interests: (1) reducing duplicative IT investments and (2) reengineering business processes. The IT dashboard initiative may ultimately provide the visibility, transparency, and accountability that are needed for an enterprise and government-wide approach to address these areas.

It is important to note that IT governance is not solely about technology. IT governance involves the management of technology, processes, and people. Ultimately, the success of IT initiatives is dependent on the people – the people that build the system, operate and maintain it, and use it. Successful adoption of new technologies and government business processes will require a strong foundation based on a policy framework and culture that discourages information and technology "silos," while encouraging information and technology sharing.

Ultimately, IT governance is about ensuring the effectiveness and efficiency of IT investments. Implementation of the Recovery Act has highlighted common IT challenges and risks faced by government agencies, because systems are not always effective and/or efficient. These include the need to ensure that (1) systems are designed to easily share information within and outside the boundaries of an organization; (2) systems are user friendly and available to the public when needed; and (3) security and privacy controls are implemented to protect sensitive information.

(3) Key IT Risk Management Challenges from an Inspector General Viewpoint

There are many risks that must be managed to ensure that our IT systems are effective and efficient. The last area I will discuss with you today is IT risk management challenges from an Inspector General viewpoint. As we implement new technologies and evaluate changes to business processes, addressing these challenges may help ensure that goals for transparency, accountability, security, and privacy are achieved.

First, implementing information security programs that are risk-based to protect the information and information systems of the government, as required by FISMA, is a key IT risk management challenge. New technologies being implemented across the government will require a careful balance between providing transparency, accountability, and visibility, while maintaining

[4] GAO Blasts Weapons Budget, The Washington Post, available at http://www.washingtonpost.com/wp-dyn/content/article/2008/03/31/AR2008033102789.html

security and privacy. Further, as the government increases reliance on contractor provided and outsourced system solutions, CIOs, IGs, and other stakeholders must work together to ensure that policy frameworks and agency information security programs are adapting to manage risks within this environment.

Secondly, strengthening our IT governance and control models is needed to ensure that we are protecting taxpayer resources and ensuring that the Federal government benefits from new technologies. Earlier, I mentioned "cloud computing" as a technology being evaluated for use in the government. There are many models of the "cloud." One model of "cloud computing" is a pay-per-use model that provides access to shared computing resources (e.g., servers, storage, software, and applications). With "cloud computing" traditional system boundaries and definitions may no longer apply. Moreover, existing policy frameworks and governance processes may need to be strengthened to ensure that sensitive information is secured and the privacy of American citizens maintained in the "cloud."

Lastly, I would like to underscore the importance of ensuring that our IT systems are supporting the Recovery Act effectively and efficiently and assisting in preventing and detecting fraud waste and abuse. The Recovery Act requires the spending of nearly $800 billion with speed to stimulate the Nation's economy. Unfortunately, this same speed leads to an environment where fraud, waste, and abuse can go undetected if our IT systems are not controlled and working in concert with other management processes.

Conclusion

The IT dashboard initiative is an important first step in providing increased visibility and accountability into the government's IT portfolio. Better collaboration between IGs and CIOs will help ensure better IT governance, successful IT projects, and better risk management. In short, this will lead to improved accountability and transparency in government. In light of the Recovery Act, we are looking for greater accountability and more transparency, and this partnership is critical to achieving these goals.

Thank you for the opportunity to speak to you on these important issues.