EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

August 8, 2011

M-11-29

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
               Director

SUBJECT: Chief Information Officer Authorities

In December 2010, the Administration released the 25 Point Implementation Plan to Reform Federal Information Technology (IT) Management.[1] The reforms are focused on eliminating barriers that get in the way of effectively managing IT programs throughout the Federal government. Too many Federal IT projects have run over budget, fallen behind schedule, or failed to deliver promised functionality, hampering agency missions and wasting taxpayer dollars.

As the Federal government implements the reform agenda, it is changing the role of Agency Chief Information Officers (CIOs) away from just policymaking and infrastructure maintenance, to encompass true portfolio management for all IT. This will enable CIOs to focus on delivering IT solutions that support the mission and business effectiveness of their agencies and overcome bureaucratic impediments to deliver enterprise-wide solutions. This memo is designed to clarify the primary area of responsibility for Agency CIOs throughout the government, as identified in the IT Reform Plan.

Agency CIOs must be positioned with these responsibilities and authorities to improve the operating efficiency of their agencies. In addition to their statutory responsibilities through the Clinger-Cohen Act[2] and related laws, under the IT Reform Plan there are four main areas in which Agency CIOs shall have a lead role:

1. **Governance.** CIOs must drive the investment review process for IT investments and have responsibility over the entire IT portfolio for an Agency. CIOs must work with Chief Financial Officers and Chief Acquisition Officers to ensure IT portfolio analysis is an integral part of the yearly budget process for an agency. The IT Reform plan restructured the investment review boards (IRBs) by requiring Agency CIOs to lead "TechStat" sessions – actionable meetings designed to improve line-of-sight between project teams and senior executives. Outcomes from these sessions must be formalized and followed-up through completion, with the goal of terminating or turning around one-third of all underperforming IT Investments by June 2012.

---

[1] http://www.cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf
[2] Public Law 104-106, Division E, Clinger-Cohen Act of 1996

2. **Commodity IT.** Agency CIOs must focus on eliminating duplication and rationalize their agency's IT investments. Agency commodity services are often duplicative and sub-scale and include services such as: IT infrastructure (data centers, networks, desktop computers and mobile devices); enterprise IT systems (e-mail, collaboration tools, identity and access management, security, and web infrastructure); and business systems (finance, human resources, and other administrative functions). The CIO shall pool their agency's purchasing power across their entire organization to drive down costs and improve service for commodity IT. In addition, enterprise architects will support the CIO in the alignment of IT resources, to consolidate duplicative investments and applications. CIOs must show a preference for using shared services as a provider or consumer instead of standing up separate independent services.

3. **Program Management.** Agency CIOs shall improve the overall management of large Federal IT projects by identifying, recruiting, and hiring top IT program management talent. CIOs will also train and provide annual performance reviews for those leading major IT programs. CIOs will also conduct formal performance evaluations of component CIOs (e.g. bureaus, sub-agencies, etc.). CIOs will be held accountable for the performance of IT program managers based on their governance process and the IT Dashboard.

4. **Information Security.** CIOs, or senior agency officials reporting to the CIO, shall have the authority and primary responsibility to implement an agency-wide information security program and to provide information security for both the information collected and maintained by the agency, or on behalf of the agency, and for the information systems that support the operations, assets, and mission of the agency. Part of this program will include well-designed, well-managed continuous monitoring and standardized risk assessment processes, to be supported by "CyberStat" sessions run by the Department of Homeland Security to examine implementation. Taken together, continuous monitoring and CyberStats will provide essential, near real-time security status information to organizational officials and allow for the development of immediate remediation plans to address any vulnerabilities.

With responsibilities for these four areas, Agency CIOs will be held accountable for lowering operational costs, terminating and turning around troubled projects, and delivering meaningful functionality at a faster rate while enhancing the security of information systems. These additional authorities will enable CIOs to reduce the number of wasteful duplicative systems, simplify services for the American people, and deliver more effective IT to support their agency's mission.

In addition, under the IT Reform Plan, Agency CIOs are required to play a cross-agency portfolio management role through the Federal CIO Council (CIOC). The CIOC charter will be amended to reflect these new responsibilities, which will allow more effective development and management of shared services, cross-agency initiatives, and governmentwide policy. Just as CIOs are tasked to find and eliminate duplicative systems in their agencies, the Council will seek opportunities to reduce duplication, improve collaboration and to eliminate waste across agency boundaries.