



UNITED STATES DEPARTMENT OF COMMERCE
The Secretary of Commerce
Washington, D.C. 20230

JUN 21 2012

MEMORANDUM FOR: Bureau Heads, Deputies, and CIOs

FROM: Rebecca M. Blank *Rebecca Blank*
Acting Secretary of Commerce

SUBJECT: Department IT Portfolio Management Strategy

On March 5th I issued a memorandum to the CIO, Simon Szykman, directing him to develop a Department IT Portfolio Management Strategy "that strengthens the ability of the Office of the CIO ... to better manage the efficiency and effectiveness of IT spending, IT decision-making, and IT systems."

Since then, we have been working with you to incorporate your input to the policy. I thank you and your staff for the serious consideration and thoughtful interactions we have had on various aspects of the policy. Our discussions have led to a better understanding by everyone. Based on the reviews of your plans to implement the policy, I am positive we will have a stronger, more effective and more efficient approach to managing the IT Portfolio of the Department. I look forward to progress updates on your implementation plan in the coming months.

With this memorandum, I am issuing the final policy developed by the CIO with input from your bureaus (attached).

Attachment

Department of Commerce IT Portfolio Management Policy

Section 1. Background

The Clinger-Cohen Act of 1996 directs heads of agencies to perform a number of responsibilities with respect to information technology^{1,2} (IT) investments, including the following:

- Design and implement in the executive agency a process for maximizing the value, and assessing and managing the risks, of the information technology acquisitions of the executive agency;
- Provide for the selection of information technology investments to be made by the executive agency, the management of those investments, and the evaluation of the results of those investments;
- [Use a process that shall] be integrated with the processes for making budget, financial, and program management decisions in the executive agency;
- Establish goals for improving the efficiency and effectiveness of agency operations and, as appropriate, the delivery of services to the public through the effective use of information technology.

Department Organization Order (DOO) 15-23 delegates authority from the Secretary to the Chief Information Officer (CIO³) to ensure the Department's compliance with the applicable provisions of the Clinger-Cohen Act of 1996. These provisions include authority associated with decisions regarding whether to continue, modify, or terminate an IT program or project based on performance of the IT investment.

OMB Memorandum M-11-29, *Chief Information Officer Authorities* (dated August, 2011), identified four areas in which Agency CIOs shall have a lead role: (1) Governance, (2) Commodity IT, (3), Program management, and (4) Information Security. Per the OMB memorandum, the rationale for identifying these additional authorities is to 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. OMB's *25 Point Plan for Reform of Federal Information Technology Management* (dated December, 2010) states that as the government moves forward with IT reforms, CIO focus must shift towards portfolio management.

OMB Memorandum M-12-10, *Implementing PortfolioStat* (dated March 2012), directs agencies to "review their respective IT investment portfolios to identify opportunities to consolidate the acquisition and management of commodity IT services, and increase the use of shared-service delivery models."

GAO Report GAO-11-634, *Federal Chief Information Officers: Opportunities Exist to Improve Role in Information Technology Management* (dated September, 2011), identified several challenges facing CIOs, including limitations on control and influence over IT budgets, commodity IT investments, and staffing decisions. These obstacles were referred to as being consistent with issues previously identified by GAO that prevented CIOs from advising and influencing their agencies in managing IT for successful outcomes – despite the broad authority that GAO finds is given to CIOs in Federal law.

GAO Report GAO-12-342SP, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue*, reviewed duplicative and overlapping investments including IT investments at several Federal agencies. Although DOC was not among the agencies reviewed, GAO found duplicative/overlapping investments at other agencies and identified frequently-cited reasons that included decentralized governance within departments and a lack of control over facilities.

¹ Unless stated otherwise, references to information technology in this policy shall generally use the definition provided in the Clinger Cohen Act, which defines IT as "any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product" and states that "The term 'information technology' includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources."

² The definition of IT in the Clinger Cohen Act does not focus solely on commodity IT or business/administrative systems, nor does it exclude mission systems.

³ In this policy, "CIO" refers to the DOC CIO unless provisions explicitly reference operating unit CIOs.

The DOC Office of the Inspector General noted in its January 2010 *Top Management Challenges* report that "... decentralization gives its CIO only limited authority over the daily management of IT security at Commerce's Operating Units and adds complexity to Department-wide information security initiatives."

In a memorandum dated 5 March, 2012, the Deputy Secretary directed the CIO to develop an IT Portfolio Management Policy that strengthens the ability to better manage the efficiency and effectiveness of IT spending across DOC. This policy serves to articulate roles and responsibilities of the DOC CIO as derived from Federal Law, flowing from delegations from the Secretary, and consistent with intent provided through OMB guidance.

Section 2. Enterprise Architecture Management

01. The CIO may define an Enterprise Architecture (EA) and a Technical Reference Model (TRM) for the Department.
 - The EA and/or TRM shall use IT architectural principles to define architectures and standards aimed at defining a "to-be" architecture for the Department, with the goal of using IT to more effectively and efficiently enable the Department's missions. The intent is for the Department's IT investments to evolve over time into a more effectively managed set of capabilities through the role of the EA and TRM compliance requirements in influencing IT investment, system development, and acquisition decisions.
 - Since the Department-level EA and TRM are meant to identify only those requirements that apply Department-wide, operating unit EAs and TRMs may (and generally will) be broader in scope than the Department-level EA/TRM. Operating unit EAs/TRMs shall be in alignment with and to be consistent with the Department-level EA/TRM.
02. The Department-level EA and TRM shall be developed in consultation with Operating Units.

Section 3. Service Catalog and Governance

01. The CIO may define a Department-level IT Service Catalog that defines generic or core IT services⁴ that shall only be provided centrally for the entire department or identified portions of the Department (e.g., the Herbert C. Hoover Building).
 - At the CIO's discretion, centralized services may be provided by an Operating Unit rather than headquarters organizations, and there may be more than one provider of central services.
 - At the CIO's discretion, the service catalog may also establish standards by which service providers must provision and/or deliver these services even in cases when they are not provided centrally.
02. Requirements for defining and implementing centralized services shall be aimed at providing improvements in effectiveness of IT spending (examples may include greater service effectiveness, better customer service, cost efficiencies, improved security, reduced risk, etc), shall be developed in consultation with Operating Units, and shall include documented service levels and associated agreements.

Section 4. IT Budget Formulation, Investment and Acquisition Review

01. While funding generally resides within Operating Units, pursuant to the CIO's oversight responsibilities, the CIO shall have discretion to review and approve IT investments and acquisitions during budget formulation and program execution.
02. The CIO shall establish IT investment and/or acquisition review thresholds (based on criteria that may include initial cost, annual cost, total lifecycle cost). Any DOC IT investment and/or acquisition that exceeds these thresholds shall be subject to review by the CIO via the Commerce IT Review Board (CITRB) or other mechanism identified by the CIO and/or the Chief Acquisition Officer.

⁴ "Services" is used in a generic way, to refer to provisioning, acquisition and/or purchasing (including but not limited to Department-wide strategic sourcing contracts) of IT products, infrastructure, or IT management/support services.

03. The CIO shall establish IT investment and/or acquisition approval thresholds (based on criteria that may include initial cost, annual cost, total lifecycle cost) above which:
 - CIO approval is required prior to submitting budget requests from DOC to OMB through the annual Presidents' Budget formulation process.
 - During program execution, any acquisition plan associated with the IT investment requires approval by the CIO.These thresholds may but need not necessarily be the same as those for IT investment/acquisition review.
04. The CIO may also carry out reviews of other DOC IT investments and/or acquisitions based on criteria other than cost thresholds, including but not limited to risk and/or mission criticality. Higher-level review mechanisms may also be established by the Secretary or Deputy Secretary to review IT investments with CIO participation for these or other reasons.
05. The CIO shall carry out oversight of IT investments via monthly reporting to the Federal IT Dashboard as well as IT investment and/or acquisition reviews, and shall be empowered to make decisions regarding whether to continue, modify, or terminate an IT program or project based on performance of the IT investment. Performance may be assessed against any of a number of objective, documented IT management criteria, including but not limited to budget/schedule/milestone performance, security and risk management, effective acquisition planning, and architectural compliance.

Section 5. IT Workforce Management

01. Offices, groups, teams, or other organizations that are responsible for providing generic IT services identified in the DOC or an Operating Unit-level IT Service Catalog shall either report to the Department Office of the CIO (OCIO), or if located outside of the management chain of the CIO shall be led by an individual who has at least 25% of his/her performance rated by the CIO or his/her delegate. This applies to Operating Unit CIOs as well as heads of organizations involved in providing generic IT services outside of Department and Operating Unit CIO management chains.
02. Advertising a position to hire an IT specialist in any organization outside of the Department OCIO or an Operating Unit OCIO requires the written approval of the CIO or his/her delegate.
03. An Operating Unit shall have no more than one individual holding the title of Chief Information Officer.

Section 6. Delegations

01. The Operating Unit CIOs will perform within their respective Bureaus the same functions assigned above to the Department CIO. The CIO may in writing delegate any portion of IT Portfolio Management responsibilities identified above to any individual Operating Unit CIOs.

Section 7. Exceptions

01. The CIO may in writing approve waivers to portions of this policy. Operating Unit CIOs may in writing approve waivers relating to portions of this policy delegated by the CIO to Operating Unit CIOs. While Operating Unit-level waivers may document exceptions to Operating Unit-level implementation of delegated portions of this policy, Operating Unit-level activities must still be consistent with Department-level activities, criteria, thresholds, unless a waiver from the Department CIO is in place.
02. This policy applies to all DOC organizations, but for USPTO applies subject to limitations of DOC headquarters involvement in USPTO management expressed in Department Organizational Order (DOO) 10-14 and elsewhere in DOC policy.
03. In order to support the Office of the Inspector General's need for independence, special consideration should be given to planning of shared infrastructure and/or services involving OIG. The need to properly maintain independence may affect the degree to which OIG can make use of or participate in such initiatives.