Congressional Research Service

Report RS21260

Information Technology (IT) Management: The Clinger-Cohen Act and the Homeland Security Act of 2002

Jeffery W. Seifert, Resources, Science and Industry Division

June 7, 2005

Abstract. The role of information technology (IT) figures prominently in the Homeland Security Act of 2002 (P.L. 107-296). Although most of these provisions are primarily focused on external information management (i.e., the department's interactions with other departments and agencies), some internal information management provisions are also included to help address the challenges of absorbing the programs, personnel, and objectives now residing in other agencies. For example, Section 103 addresses an aspect of federal management, the creation of a Chief Information Officer (CIO), which was established for agencies under the Clinger-Cohen Act of 1996. The law also outlines IT management duties for some of the Under Secretaries. Compared in relation to the Clinger-Cohen Act, the information technology management provisions raise some potential oversight issues including the appointment and reporting requirements of the department-level CIO, overlapping IT management responsibilities between various departmental officials, and possible national security exemptions from Clinger-Cohen requirements.

Order Code RS21260
Updated June 7, 2005

Information Technology (IT) Management: The Clinger-Cohen Act and the Homeland Security Act of 2002

Jeffrey W. Seifert
Analyst in Information Science and Technology Policy
Resources, Science, and Industry Division

Summary

The role of information technology (IT) figures prominently in the Homeland Security Act of 2002 (P.L. 107-296). Although most of these provisions are primarily focused on external information management (i.e., the department's interactions with other departments and agencies), some internal information management provisions are also included to help address the challenges of absorbing the programs, personnel, and objectives now residing in other agencies. For example, Section 103 addresses an aspect of federal management, the creation of a Chief Information Officer (CIO), which was established for agencies under the Clinger-Cohen Act of 1996. The law also outlines IT management duties for some of the Under Secretaries. Compared in relation to the Clinger-Cohen Act, the information technology management provisions raise some potential oversight issues including the appointment and reporting requirements of the department-level CIO, overlapping IT management responsibilities between various departmental officials, and possible national security exemptions from Clinger-Cohen requirements. This report will be revised as congressional action requires.

Background

Previous to the current focus on homeland security, congressional policymakers have frequently expressed a strong interest in government reform and improved management of public resources, and they have acted to improve several areas of government management. Some examples of congressional action over the last several years include the Chief Financial Officers (CFO) Act of 1990, the Government Performance and Results Act (GPRA) of 1993,[1] the Federal Acquisition Streamlining Act (FASA) of 1994,

[1] See also: CRS Report RS20257, *Government Performance and Results Act: Brief History and Implementation Activities During the 106th Congress*, by Genevieve J. Knezo.

the Federal Acquisition Reform Act (FARA) of 1996, and the Information Management and Reform Act (ITMRA) of 1996.[2]

A year after passage, FARA and ITMRA were renamed the Clinger-Cohen Act of 1996 in the FY1997 Omnibus Consolidated Appropriations Act, P.L. 104-208. Since 1997 the provisions of the Clinger-Cohen Act have served as the primary statutory basis for federal information technology management issues. Among the major provisions of the Clinger-Cohen Act are the establishment of department-level chief information officers, the elimination of the General Service Administration's primary role in setting policy and regulation for federal information technology procurement/acquisition, the deployment of information security practices, and the establishment of two pilot programs to test alternative acquisition approaches (Share-in Savings and Solutions-Based Contracting).[3]

The ongoing interest in homeland security issues has brought further attention to government information technology management. Information technology has been cited not only as a means to more efficiently manage an agency's internal operations, but also to facilitate activities such as information sharing among departments as well as between federal, state, and local government.[4] Consequently, some provisions were included in the Homeland Security Act of 2002 that position information technology management practices as a means to achieve homeland security goals.

Department of Homeland Security

In the aftermath of the terrorist attacks of September 11, 2001, Congress passed legislation to create a department for homeland security. While P.L. 107-296 contains many provisions, the overall intent of the law is to provide for the consolidation and coordination of federal government programs and activities to combat terrorism.

The role of information technology figures prominently in the Homeland Security Act of 2002. However, most of the references to information technology in P.L. 107-296 are used to delineate the department's role as a facilitator of standards, a leader in establishing priorities for research and procurement, and a provider of advice and information to other departments in the area of homeland security applications. For example, Section 301 includes provisions for a Directorate of Science and Technology. Generally, these provisions call for developing a system for sharing key homeland

---

[2] FARA and ITMRA were passed as Sections D and E, respectively, of the National Defense Authorization Act for Fiscal Year 1996, P.L. 104-106.

[3] For additional information regarding the Clinger-Cohen Act, see CRS Report RL30661 *Government Information Technology Management: Past and Future Issues (The Clinger-Cohen Act)* by Jeffrey W. Seifert.

[4] General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy*, GAO-02-811T, 7 June 2002; Nick Wakeman, "Homeland Security IT Spending Could Top $2 Billion," *Washington Technology*, 7 June 2002, [http://www.washingtontechnology.com/news/1_1/daily_news/18392-1.html]; "New Homeland Security Department Aims for IT Compatibility," *Washington Technology*, 7 June 2002, [http://www.washingtontechnology.com/news/1_1/daily_news/18390-1.html].

security research and technology developments and opportunities with appropriate federal, state, local, and private sector entities. Title V, Emergency Preparedness and Response, directs the department to develop "comprehensive programs for developing interoperative communications technology, and helping to ensure that emergency response providers acquire such technology."

Following from the department's mission to coordinate and lead efforts to reduce the vulnerability of the United State to terrorism, these provisions are primarily focused on external information management (i.e., the department's interactions with other departments and agencies) rather than explicitly describing or defining the department's management of its own information technology resources. However, a significant challenge for the department at its outset was to absorb the programs, personnel, and objectives then residing in other agencies. To that end, some provisions regarding department-level internal information technology management were included and are discussed in relation to the Clinger-Cohen Act below.

The Clinger-Cohen Act and Homeland Security

The Clinger-Cohen Act currently serves as the primary legislative guidance for most executive departments and agencies regarding information technology management. Where the Homeland Security Act is silent, it is anticipated that the relevant provisions of the Clinger-Cohen Act will apply to the Department of Homeland Security. However, there are some provisions in the Homeland Security Act that explicitly outline information technology management practices for the new department, which are in contrast to those followed by most other departments. These differences could be relevant to oversight efforts as Congress continues to evaluate the implementation of the Homeland Security Act.

Chief Information Officer. Section 5125, Subtitle A, Title LI of the Clinger-Cohen Act mandates the creation of a CIO in each federal agency. The duties of the CIO as described in the act are to provide information management advice and policy to the agency head; develop, maintain, and facilitate information systems; and evaluate, assess, and report to the agency head on the progress made developing agency information technology systems.

Appointment and Reporting Requirements of the Chief Information Officer. P.L. 107-296 includes a provision for the establishment of a department-level chief information officer. Section 103 stipulates that the CIO will be appointed by the President. This contrasts with the Clinger-Cohen Act, under which department-level CIOs are appointed by their respective department Secretaries. The CIO of a department is an Executive Level IV position. The Office of Management and Budget (OMB) Memorandum M-96-20 *Implementation of the Information Technology Management Act of 1996*, the OMB guidelines for implementation of the Clinger-Cohen Act, states that "each agency head is expected to select and position a CIO to ensure the effective acquisition and use of IT and to carry out the agency's information resources management responsibilities."[5] However, OMB Memorandum M-96-20 has been superceded by OMB Circular A-130, which is silent on this issue.

[5] See [http://www.whitehouse.gov/omb/memoranda/m96-20.html].

Section 703 also states that the department-level CIO is to report to the Secretary of Homeland Security or some other official the Secretary designates. The Clinger-Cohen Act stipulates that department-level CIOs are to report directly to their respective department Secretaries.

Overlapping Information Technology Management Responsibilities. Although Section 703 establishes a department-level CIO for the new department, Section 701 also includes provisions making the Under Secretary for Management responsible for management and administration of the new department's information technology and communications systems. It is unclear how the overlapping responsibilities for information technology systems between the department-level CIO and the Under Secretary are mediated in practice. However, both the DHS Inspector General (IG) and the Government Accountability Office (GAO) have released reports critical of DHS IT management structures and practices. Among the problems they identified, both organizations highlighted the lack of centralized authority over IT assets and personnel as a significant weakness of the DHS CIO position.[6] Congress may choose to address this issue, in part, by approving a FY2006 budget for DHS that emphasizes initiatives and management structures that centralize control over IT resources within the office of the DHS CIO.[7]

National Security Exemptions. Subtitle E, National Security Systems, of the Clinger-Cohen Act states that most of the provisions of the law do not apply to national security systems.[8] National security systems are defined as those which involve intelligence activities, cryptography, command and control, weapon systems, or other information systems used in carrying out the defense of the nation. Generally, this provision in the act was included to give those agencies that handle classified and sensitive information greater flexibility in how they acquire and procure information technology.

The Department of Homeland Security includes some of the activities described in Subtitle E. To that end, the Homeland Security Act does provide some exemptions similar to those provided in the Clinger-Cohen Act. Section 3533 exempts national security systems from oversight by the Director of OMB for the development and implementation of information security standards. Section 3538 goes on to state that "Nothing in this act (including any amendment made by this act) shall supersede any authority of the Secretary of Defense, the Director of Central Intelligence, or other agency head, as authorized by law and as directed by the President, with regard to the operation, control, or management of national security systems, as defined by section 3532(3) of title 44, United States Code." At this time it is still unclear whether the department's evolving

---

[6] Department of Homeland Security, Office of the Inspector General, *Improvements Needed to DHS' Information Technology Management Structure*, OIG-04-30, July 2004, p. 21; Government Accountability Office, *Department of Homeland Security: Formidable Information and Technology Management Challenge Requires Institutional Approach*, GAO-04-702, August 2004, p. 15.

[7] Alice Lipowicz, "Consolidating the Homeland: Bush Budget Request Pushes DHS Integration Efforts," *Washington Technology*, 21 March 2005, [http://www.washingtontechnology.com/news/20_6/security/25825-1.html].

[8] It is important to note that national security agencies also have CIOs.

role will result in being significantly different from existing national security agencies and departments; and if new security responsibilities will qualify as a national security system.