CIO Update: The Expanding Responsibilities

L. John Michel
Information Resources Management College, National Defense University

It has been five years since the 1996 Clinger-Cohen Information Technology Management Reform Act was enacted mandating that all federal executive agencies have chief information officers (CIOs). Since then additional legislation and directives have expanded the role and responsibilities of federal CIOs. This article discusses how in today's world of e-commerce and e-government, federal CIOs must tackle infrastructure, architectures, information assurance, acquisition, software, information security, capital planning, human resource management, education, and other initiatives designed to improve the management of information technology resources.

The closing general session of the 1997 Software Technology Conference (STC) focused on the chief information officer (CIO) roles and responsibilities, and the 1966 Clinger-Cohen Information Technology Management Reform Act mandating that all federal executive agencies have CIOs. Attendees heard the Department of Defense (DoD) perspective from Cythnia Rand, who at that time was the principal director for Information Management, assistant secretary of defense for Command Control Communications and Intelligence (C3I). The CIO of Hewlett-Packard and the vice president of Strategic Business Initiatives from EDS gave industry's perspective.

The myth that preoccupies information systems executives is that CIO stands for "career is over [1]." Sitting in the ballroom of the Salt Place Convention Center in Salt Lake City during the STC conference, an attendee next to me questioned the need for the software community to understand the Clinger-Cohen act and the position of CIO. That person was oblivious to the transformation. Information intensive systems and the advances in information technology (IT) were fueling the revolution in military affairs within DoD and the revolution in business affairs in the federal government. As those revolutions continue today, CIOs' responsibilities are increasing with the passage of additional legislation and issuance of directives to meet the challenges of "e-government." CIOs are charged with a wide-ranging set of duties that provide the threaded connection needed to manage cyber space.

For that person who was sitting next to me, I hope that by the end of this article you see that in an ever-increasing information-intensive environment, CIOs have a crucial seat at the table. This article begins by reviewing the original act in order to set the foundation for analyzing the additional directives and legislation that have expanded the responsibilities of federal CIOs.

The Clinger-Cohen Act Revisited

The Clinger-Cohen Act, Division E of the fiscal year 1996 Defense Authorization Act, Public Law 104-106 (formerly the Information Technology Management Reform Act) was signed by President Clinton in 1996. It repealed the 1965 Brooks Act and directed federal agencies to put modern IT management frameworks into effect. The act established the position of the CIO for the executive agencies. In chartering this position, the framers of the act set forth certain responsibilities that CIOs should have.

> *"CIOs' responsibilities are increasing with the passage of additional legislation and issuance of directives to meet the challenges of e-government."*

> "(1) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that IT is acquired and information resources are managed for the executive agency in a manner that implements the policies and procedures of this division, consistent with chapter 35 of title 44, United States Code, and the priorities established by the head of the executive agency;
> (2) Developing, maintaining, and facilitating the implementation of a sound and integrated IT architecture for the executive agency; and
> (3) Promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency [2]."

Additionally, the act tasked the CIO with monitoring the performance of IT programs. Based on applicable performance measurements, the CIO would advise the head of the agency regarding whether to continue, modify, or terminate a program or project. The act stipulated that CIOs assess the requirements for agency personnel regarding knowledge and skill in information resources management, and develop strategies and specific plans for hiring, training, and professional development [3].

Following are other important components of the act to remember:

1. It repealed the requirement that agencies go through the General Services Administration for IT acquisitions.
2. Office of Management and Budget (OMB) has oversight control over agency IT spending through the budgeting process.
3. Agencies were required to create a process for maximizing the value and assessing and managing the risk of the IT acquisition.
4. Agencies had to develop performance measurements for IT that will measure how well the technology supports the programs of the agency.
5. Standards and guidelines are compulsory and binding to improve the efficiency of operation or security, and

privacy of federal computer systems.
6. Agencies acquire IT incrementally through the use of modular contracting.
7. Procurement protest authority now resides with the U.S. comptroller general and the General Accounting Office (GAO).

Two terms in the act are worth reviewing: IT and ITN National Security Systems (NSS). Clinger-Cohen defines IT in such a way that it encompasses business, command, control (C2), communications (C3), computer (C4), and intelligence (C4I) systems, and embedded systems:

> "…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. [It] includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources [4]."

The Clinger-Cohen Act defines a NSS as "… any telecommunications or information system operated by the United States government, the function, operation, or use of which:
1. Involves intelligence activities;
2. Involves cryptologic activities related to national security;
3. Involves command and control of military forces;
4. Involves equipment that is an integral part of a weapon or weapons system; or
5. Is critical to the direct fulfillment of military or intelligence missions [5]."

Even though the act does not apply to NSS, there are numerous exceptions that bring these systems under the purview of the CIO. Section 5123 Performance- and Results-Based Management, Section 5126 Accountability, and Sections 5112 and 5122 Capital Planning and Investments Control all apply to NSS [6]. This was reinforced in a 1997 Office of the Secretary of Defense memorandum that stated, "Recent guidance from OMB places added emphasis on managing investments, to include weapons systems [7]."

For our discussion on the responsibilities of the CIO, it is important to remember that the major responsibilities, Section 5125, apply to the NSS. Thus the DoD CIO provides advice and assistance to the secretary of defense to ensure that NSS and IT resources are acquired consistent with law and policy. As we shall see this advice and assistance role has been incorporated into the acquisition life cycle.

Clinger-Cohen was a foundation for improving agency performance. Throughout the first years of implementation, CIOs worked to overcome the challenges faced with fulfilling new legislative requirements. Although Clinger-Cohen mandated enterprise architectures, it did not specify underlying components of standards and interoperability. In DoD, publication of Joint Vision (JV) 2010 established technological innovation as a key enabler and interoperability as the foundation; legislation was enacted that enables the DoD CIO to move from JV 2010 to JV 2020.

Expanding the Responsibilities of the DOD CIO

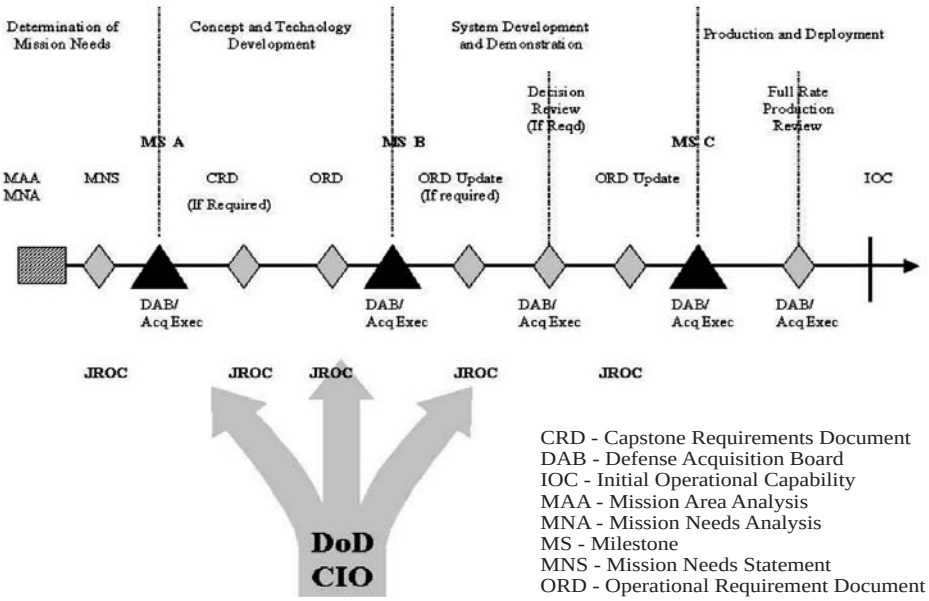
JV 2020 relies on IT and information systems to achieve its goal of full spectrum dominance through the operational concepts of dominant maneuver, precision engagement, focused logistics, and full dimensional protection. To achieve this dominance requires information superiority, joint C2 information operations, and a foundation of interoperability. Business applications (logistics, transportation, medical, and personnel) are certainly key enablers in JV 2020. Under the general responsibilities defined by Clinger–Cohen, the CIO is charged with ensuring that the information infrastructure will support full spectrum dominance. In order to do this the CIO must now address issues of interoperability and standardization.

In October of 1998, legislation was enacted that added additional responsibilities for the DoD CIO and the CIOs of the military departments. Public Law 105-261, Strom Thurmond National Defense Authorization Act for fiscal year 1999 set forth, in addition to the responsibilities in the Clinger-Cohen Act, the following:
1. Review and provide recommendations to the secretary of defense on DoD budget requests for IT and NSS.
2. Ensure the interoperability of IT and NSS throughout the DoD.
3. Ensure that IT and NSS standards that will apply throughout the DoD are prescribed.
4. Provide for the elimination of duplicate IT and NSS within and between the military departments and defense agencies.

Ensuring interoperability of IT and NSS places the CIO in the forefront of building the foundation for JV 2020. The law also strengthens the CIO role in the requirements and acquisition process by providing a mechanism for budget review and recommendations.

To ensure a robust infrastructure, the CIO is a key player in requirements and acquisition process of the systems that will provide full spectrum dominance. Figure 1 depicts the DoD CIO's sphere of influence throughout the acquisition life cycle, which is ensconced in the charter of the Joint Requirements Oversight Council. "The Director of Architecture and Interoperability in the Office of the DoD CIO will serve the Joint Requirements Oversight Council (JROC) in an advisory role on Information

Figure 1: *The DoD CIO Role in the Acquisition Life Cycle*



Defense Department CIOs

Department of Defense
Assistant Secretary of Defense (C3I)/Chief Information Officer
John P. Stenbit
http://www.c3i.osd.mil/

Joint Community
Director, Command, Control, Communications, and Computer Systems (J-6)
LTG Joseph Kellogg
www.dtic.mil/jcs/ccrc/leadership.html

Department of the Army
Director of Information Systems for Command, Control, Communications, and Computers (DISC4)
LTG Peter Cuviello
www.army.mil/disc4/index.html

Department of the Navy
Chief Information Officer
Mr. Dan Porter
204.222.128.9/doa-cio/cio-lib.html

Marine Corps
Director Command, Control. Communications, and Computers (C4)
Brig Gen Robert F. Shea
issb-www.1.mqg.usmc.mil/cic/index.html

Department of the Air Force
Assistant Secretary for Acquisition
Dr. Lawrence Delaney
www.cio.hq.af.mil

Table 1: *Defense Department CIOs*

Technology, including National Security Systems. In addition, the DoD CIO will support JROC responsibilities for developing and validating the operational view of integrated operational concepts/architectures and related products as well as ensuring interoperability [8]."

As the chairman of the Joint Chiefs of Staff Instruction 3170.01b dated April 15, 2001 reiterates, the DoD CIO is responsible for ensuring the interoperability of IT and NSS throughout the DoD. The DoD CIO will ensure that IT and NSS standards that will apply throughout the department are prescribed, and provide for elimination of duplicate IT within and between the military departments and defense agencies. Through these recommendations, the CIO provides the advice to senior management personnel of the executive agency to ensure that IT is acquired in a manner that implements the policies and procedures of the Clinger-Cohen Act and Public Law 105-106.

The Global Information Grid (GIG) binds the architectural mandate of Clinger-Cohen with the interoperability and standards directives of Public Law 105-106. Through the GIG, the DoD CIO is implementing a sound and integrated architecture, which will provide globally interconnected information capabilities, associated processes, and personnel for collecting, storing, processing, disseminating, and managing information on demand to warfighters, policy-makers, and supporters [9]. The GIG supports all DoD, national security, and related intelligence community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides interfaces to coalition, allied and non-DoD users, and systems [10]. The acquisition of GIG components will see a convergence of technology that will support the next leap in the revolution in military affairs and the revolution in business affairs.

Within the constructs of a defined architecture, the DoD CIO ensures the acquisition of interoperable systems that will set the foundation for full spectrum dominance. For the GIG to provide the right information at the right time to the right warfighter in the right format requires a high level of assurance. Thus it is no surprise that information assurance is one of the overarching policy considerations in the GIG architecture.

Assuring the Information Infrastructure

> "There's a war out there old friend, a world war, and it's not about who's got the most bullets. It's about who controls the information – about how we see and hear, how we work, what we think. It's all about the Information … [11]"

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems [12]. As a result of advances in IT and the necessity of improved efficiency, the physical and logical separate systems of the infrastructures have become increasingly automated and interlinked. With an interoperable GIG as a foundation for achieving full spectrum dominance, successful implementation requires assurance. Presidential Decision Directive 63 tasks the CIOs with critical information infrastructure protection.

> Every department and agency of the federal government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency CIO shall be responsible for information assurance. Every department and agency shall appoint a chief infrastructure assurance officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems [12].

Within the DoD, the CIO is also designated as the CIAO. In most of the other federal agencies, a separate position or office of critical infrastructure protection has been created thus separating the protection of the information infrastructure from the physical infrastructure. However, in looking at the organizational structure under the DoD CIO, we find that reporting to the deputy assistant secretary of defense for Security and Information Operations are the Infrastructure and Information Assurance Directorate and the Directorate for Critical Infrastructure Protection. Thus, even within the DoD the policy organizations for the physical and information infrastructures are in distinctly separate office elements.

Thus with the issuance of Presidential Decision Directive 63, President Clinton placed the CIO at the forefront of information assurance and in some cases critical infrastructure protection within the federal government. For the critical networks within the information infrastructure and the information grid, security is a primary concern. Clinger-Cohen requires that the head of the executive agency shall ensure that the information security policies and practices of the agency are adequate. But, the act does not assign this responsibility for security directly to the CIO; that comes in subsequent legislation.

Linking Assurance and Security

The link between information assurance and information security is promulgated in the most recent piece of legislation expanding the responsibilities of CIOs. The Floyd D. Spence National Defense Authorization Act for fiscal year 2001 incorporates information security into federal information policy. In doing so, it spells out relationships between the CIO and head of the agency regarding the establishment of agency policy, procedures, and control techniques that will afford sufficient security protection commensurate with the risk. The law makes numerous references to the Clinger-Cohen Act of 1996 and establishes a link between tenets such as accountability,

architecture, and security by delegating to the CIO the following authority:

1. Designate a senior agency information security official who shall report to the CIO or a comparable official.
2. Develop and maintain an agency-wide information security program.
3. Ensure that the agency effectively implements and maintains information security policies, procedures, and control techniques.
4. Train and oversee personnel with significant responsibilities for information security with respect to such responsibilities [13].

An important aspect of the legislation is that it requires the agency CIO, in coordination with senior agency officials, to periodically evaluate the effectiveness of the agency information security program, including the testing control techniques. The law further stipulates the each agency must develop an agency-wide information security program, and that the director of the OMB is tasked with approval and annual review.

The annual review process must be done with the program officials in consultation with the CIO. For the DoD and the Central Intelligence Agency (CIA), the approval and review authority rests with the secretary of defense and the director CIA. Finally, the law requires that each agency, in consultation with the CIO, shall include as part of the performance plan the resources and time required to implement the program based on a risk assessment of the agency.

This most recent piece of legislation forms the link between the security requirements of Clinger-Cohen and the assurance mandates of the Presidential Decision Directive 63. With this most recent legislation, we have seen that the responsibilities of federal CIOs have increased dramatically in a relatively short period of time. Today the CIO is facing such technology challenges as convergence and wireless, while providing assurance and security. To harness efficiencies across agencies, the question is begging: Does the federal government need an IT czar?

The Federal IT Czar

The speculation in Washington, D.C., is that President Bush will appoint a federal CIO. The Gartner Group has stated that "due to the transformational role of IT on government – Gartner believes that e-government transformation will eliminate at least 30 percent of the current government agencies. Gartner recommends that the new administration create a cabinet-level position within the executive office of the president to bring unity to the e-government movement. It is critical that the federal CIO be positioned as a key player in e-government and technology-related public policy. The president and the CIO should operate in tandem, much like successful chief executive officer (CEO)/CIO models in the private sector [14]."

Gartner Group is not the only lobby for the creation of this position. Sen. Robert Bennett (R-Utah) speaking at the U.S. Chamber of Commerce meeting "Cyber Security: The Real Y2K Challenge" stated, "The numerous legislative and agency efforts to address cyber security may need the guidance of a single 'chief information officer' to coordinate the government's cross agency and trans-industry security measures [15]."

From across the political aisle, Rep. Jim Turner (D-Texas) introduced legislation that would create the executive-level position and codify the executive order that created the interagency CIO Council [16]. There is bipartisan support as well, Sens. Fred Thompson (R-Tenn.) and Joe Lieberman (D-Conn.) chairman and ranking minority member on the Senate Governmental Affairs Committee, respectively, have expressed support for the concept [17]. Even with Congress, the GAO, and respected practitioners pushing, it is still questionable as to whether President Bush will establish an executive level IT position, a federal CIO.

Calls for a federal IT czar reinforce the criticality throughout government of the roles and responsibilities of CIOs. The continued explosion of IT in the revolution of government affairs places the CIO at the table with the CEO and the chief financial officer. The CIO ensures that technology provides seamless governmental operations and services. Facing issues in recruitment and retention, outsourcing, architecture, assurance, security, and resource management, clearly CIO does not mean, "career is over." To that individual who was sitting next to me at STC 1997, I hope you see the essential role of the CIOs in the age of e-government.

The views in this article are those of the author and do not reflect the official policy or position of the National Defense University, the DoD, or the U.S. government.◆

References

1. Baatz, E. B. "The Truth About Turnover." CIO Magazine. 1 Nov. 1996.

2. Section 5125. Agency Chief Information Officer. (b) General Responsibilities. Clinger-Cohen Act, Division E of the FY96 Defense Authorization Act, Public Law 104-106.
3. Section 5125. Agency Chief Information Officer. (c) Duties and Qualifications. Clinger-Cohen Act, Division E of the FY96 Defense Authorization Act, Public Law 104-106.
4. Section 5002. Definitions (3) Information Technology. Clinger-Cohen Act, Division E of the FY96 Defense Authorization Act, Public Law 104-106.
5. Section 5142. National Security System Defined (a) Definition. Clinger-Cohen Act, Division E of the FY96 Defense Authorization Act, Public Law 104-106.
6. Section 5141. Applicability to National Security Systems (b) Exceptions. Clinger-Cohen Act, Division E of the FY96 Defense Authorization Act, Public Law 104-106.
7. OSD Memorandum. Requirements for Compliance with Reform Legislation for Information Technology (IT) Acquisitions (Including National Security Systems), 1 May 1997.
8. Charter of the Joint Requirements Oversight Council, Chairman of the Joint Chiefs of Staff Instruction 5123.01A, 8 Mar. 2001.
9. OSD Memorandum. Global Information Grid, 22 Sept. 1999.
10. OSD Statement. Global Information Grid, 2 May 2001.
11. Sneakers. MCA Universal Pictures. 1992.
12. White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 1998.
13. Section 3534. Federal Agency Responsibilities. Subchapter II–Information Security, SEC. 1061. Coordination of Federal Information Policy, Subtitle G–Government Information Security Reform, Title X, National Defense Authorization, Fiscal Year 2001, Public Law 106-398.
14. Caldwell, French, and Judith Carr, eds. Mr. President, Appoint a Federal CIO. Note Number: TG-12-8984, The Gartner Group, 18 Mar. 2001.
15. Krebs, Brian. "Federal CIO Needed for Web Security." Newsbytes, Daily News, Computer User.Com. 15 May 2001.
16. Trimble, Paula Shaki. "New push for federal CIO." Federal Computer Week 29 May 2000.
17. Wait, Patience. "Prospect of Federal CIO Still Lingers In the Wings." Washington Technology Vol. 15 No. 21. 5 May 2001.

About the Author

L. John Michel is a professor of Systems Management at the Information Resources Management College, the National Defense University. Currently, he manages the course "Assuring the Information Infrastructure." He formerly managed "Advanced Software Acquisition Management" and "Software Management for Executives." He has over 22 years experience in programmatic aspects of software intensive systems in the command and control, intelligence, and personnel communities. He has bachelor's and master's degrees in business administration from the University of Georgia.

Information Resources Management College
National Defense University
Fort McNair, DC 20319
Phone: (202) 685-2062
Fax: (202) 685-3974
E-mail: michell@ndu.edu