

Report for Congress

Received through the CRS Web

Federal Chief Information Officer (CIO): Opportunities and Challenges

Updated July 2, 2002

(name redacted)
Analyst in Information Science and Technology Policy
Resources, Science, and Industry Division

Federal Chief Information Officer (CIO): Opportunities and Challenges

Summary

Debate over the creation of a federal Chief Information Officer (CIO) position has ebbed and flowed over the past five years as Congress has sought to address government information technology (IT) management issues. In private sector organizations, a CIO is often a senior decisionmaker providing leadership and direction for information resource development, procurement, and management, with a focus on improving efficiency and the quality of services delivered. Originally considered in an early draft of the Clinger-Cohen Act in 1995 (P.L. 104-106), the idea of a single federal CIO was dropped in favor of creating CIO positions within the executive agencies. The mixed results of agency-level CIOs, combined with a growing interest in better managing government IT resources, has renewed attention in this issue. Efforts to coordinate electronic government (e-government) initiatives has also led some observers to call for an “e-government czar” or a federal CIO.

During the 106th Congress a number of lawmakers made proposals to establish a federal CIO. In the House of Representatives one bill (H.R. 4670, Turner) would have established a federal CIO in an office outside of the Office of Management and Budget (OMB). A second bill (H.R. 5024, Davis) had similar provisions but also provided a federal CIO with a broad mandate and budget authority to carry out federal IT projects, and the power to coordinate and execute government-wide information security efforts. Neither bill was passed in the last Congress. In May 2001 a Senate bill was introduced (S. 803, Lieberman), which included many of the House bills’ provisions as well as new ones such the creation of a Federal IT Training Center. A companion House bill (H.R. 2458, Turner) was introduced in July 2001. On March 21, 2002, the Governmental Affairs Committee reported S. 803 (now renamed the E-Government Act of 2002) with an amendment. The Senate passed the bill unanimously on June 27, 2002.

Although the Bush Administration has opposed creating a separate federal CIO, in June 2001 OMB announced the creation of a new position, the Associate Director of Information Technology and E-Government, who will report to the Deputy Director of Management (DDM) at OMB. The DDM, will be the federal CIO.

Despite the OMB announcement, some policymakers suggest that many issues remain unresolved. One issue is the organizational placement of the position. There is disagreement over whether the federal CIO should be placed in OMB or if a new office should be established within the White House.

A second issue is the scope of responsibility of the position. Some proponents suggest that the federal CIO should coordinate information security issues. Critics argue that individual agencies may believe they have a reduced obligation or will devote fewer resources to information security at a time when threats to information resources are climbing. Another area of concern is budgetary authority. Many observers consider some control over funding of IT projects critical to the success of a federal CIO, either by controlling a portion of the various agencies’ budgets for IT projects or providing the federal CIO with a fund to support interagency projects.

Contents

Background	1
Recent Legislative Proposals for a Federal CIO	3
106 th Congress	3
S. 1993 (Thompson), Government Information Security Act	3
H.R. 4670 (Turner), Chief Information Officer of the United States Act of 2000	4
H.R. 5024 (Davis), Federal Information Policy Act of 2000	4
The 2000 Presidential Campaign	4
107 th Congress	5
H.R. 2458 (Turner), E-Government Act of 2001	6
S. 803 (Lieberman), E-Government Act of 2002	7
Issues	7
Should There Be a Single Federal CIO?	7
Where Should a Federal CIO be Organizationally Located?	9
Potential Responsibilities of a Federal CIO	10
Information Security	10
Budgetary Authority	11
Appendix A: Legislation in the 106 th Congress	12
S. 1993 (Thompson), Government Information Security Act	12
H.R. 4670 (Turner), Chief Information Officer Act of the United States of 2000	12
H.R. 5024 (Davis), Federal Information Policy Act of 2000	13
Appendix B: Legislation in the 107 th Congress	14
H.R. 2458 (Turner), E-Government Act of 2001	14
S. 803 (Lieberman), E-Government Act of 2002	17
Additional Reading	20

Federal Chief Information Officer (CIO): Opportunities and Challenges

Background

Debate over the creation of a federal Chief Information Officer (CIO) position has ebbed and flowed over the past five years as Congress has sought to address government information technology (IT) organizational and management issues. In private sector organizations with a CIO, this person serves as the senior decisionmaker providing leadership and direction for information resource development, procurement, and management, with a focus on improving efficiency and the quality of services delivered. The possibility of creating a federal CIO, to be located in the Office of Management and Budget (OMB), was originally considered in an early draft of what became the Clinger-Cohen Act in 1995 (P.L. 104-106). However, the idea of a single federal CIO was dropped in favor of creating CIO positions within the executive agencies in the final version of the law. The mixed results of agency-level CIOs, combined with a growing interest in better managing government technology resources, brought renewed attention to creating a national CIO position during the 106th Congress. In addition, the recent piecemeal efforts to move governmental functions and services online has led some observers to call for an electronic government (e-government) “czar” or a federal CIO to coordinate these efforts.¹

During the mid-1990s, Congress considered several bills focusing on governmental reform and improved management of public resources. The option of establishing a federal CIO was one of several proposals to address these problems. The success of CIOs in the private sector is often cited as an example for government to follow. However, the interest in establishing CIOs in the federal government was generated by the experience of local and state governments. At the time forty states had some form of a CIO operating in a policy capacity, as did several major cities. For many, their experience demonstrated that there was a need for someone to articulate a “vision” of information resources that helped coordinate agency activities and goals rather than reinforce the artificial “stovepipes” that separated them.

However, the idea of a federal CIO was dropped in favor of agency-level CIOs following testimony at a July, 1995 Senate Governmental Affairs Committee hearing. At this hearing, a number of arguments were made in favor of eliminating the single federal CIO provisions in the Clinger-Cohen Act. Some critics of the proposal argued that the operational nature of the CIO position (i.e., the development

¹See CRS Report RL30745, *Electronic Government: A Conceptual Overview*, by (name red acted) for an in-depth discussion of the policy issues affecting the development and implementation of e-government initiatives.

of technical standards, determining the applicability of procurement laws, and maintenance of performance and efficiency indicators) was a poor fit with the traditional policy role of OMB. Other critics argued that creating a federal CIO was adding another layer of bureaucracy and centralizing decisionmaking procedures. They contended that it was counterproductive to the purpose of the Clinger-Cohen Act, which was to decentralize decisionmaking processes and purchasing decisions away from the General Services Administration (GSA) to the individual executive agencies. A third argument made by some critics at the time was that the role of a federal CIO was too big for any one person or agency to handle. Proponents of this view noted that the size of the Department of Defense alone was larger than some state governments, and that cross-agency groups focusing on specific problems would be a more effective approach. In light of this opposition, Congress decided to instead designate a CIO in each of the major executive branch agencies. These agency-level CIOs were tasked with the following responsibilities:

- (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 information technology is acquired and information resources are managed for the executive agency in a manner that is 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 information technology 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

Following the passage of P.L. 104-106, President Clinton created the Chief Information Officers Council. Established by Executive Order 13011, *Federal Information Technology*, on July 16, 1996, it serves as “the principal interagency forum to improve agency practices on such matters as the design, modernization, use, sharing, and performance of agency information resources.”³ The CIO Council is comprised of the CIOs and Deputy CIOs from twenty-eight federal departments and agencies.⁴ The Deputy Director for Management for the Office of Management and Budget (OMB) serves as the Chair of the CIO Council and the Vice Chair is elected from the membership. The CIO Council meets monthly and has six committees to

²P.L. 104-106, Division E, § 5125b.

³[<http://www.npr.gov/library/direct/orders/27aa.html>]

⁴CIO Council membership also includes two representatives from the smaller federal agencies, liaisons to other executive councils, committees and boards, including the Chair of the Information Technology Resources Board and representatives from the Chief Financial Officers Council and the Procurement Executive Council. In addition, a representative from the Office of Science and Technology Policy and representatives from OMB's Office of Information and Regulatory Affairs are members of the Council. <http://www.cio.gov/docs/about.htm>

address specific information technology management concerns such as enterprise interoperability, security and privacy, and e-government. The committees work to help facilitate the growth of government standards, share best practices, and help agencies work to be in compliance with reform legislation such as the Government Performance and Results Act (GPRA). The Council's materials are sometimes used by the General Accounting Office (GAO) to help inform its methodology when evaluating the information technology management progress of various agencies.⁵ The Council also has worked with the Office of Personnel Management (OPM) to develop special pay rates for hard-to-hire IT professionals.⁶

Recent Legislative Proposals for a Federal CIO

During the 106th Congress (and the concurrent Presidential campaign) a number of policymakers made proposals regarding the establishment of a federal CIO. While none of these bills passed, new bills have been introduced during the first half of the 107th Congress. A summary of the major provisions of the relevant bills is listed below, with a more comprehensive overview provided in Appendix A.

106th Congress

S. 1993 (Thompson), Government Information Security Act.

- Requires the Director of the Office of Management and Budget to establish government-wide policies for the management of programs that: (1) support the cost-effective security of Federal information systems by promoting security as an integral part of each agency's business operations; and (2) include information technology architectures as defined under the Clinger-Cohen Act of 1996.
- Requires such policies to: (1) be founded on a continuous risk management cycle; (2) implement controls that adequately address the risk; (3) promote continuing awareness of information security risks; (4) continually monitor and evaluate information security policy; and (5) control effectiveness of information security practices.
- Outlines information security responsibilities of each agency, including the development and implementation of an agency-wide security plan for the operations and assets of such agency.

⁵See General Accounting Office, *Information Technology Management: SBA Needs to Establish Policies and Procedures for Key IT Processes*, GAO-AIMD-00-170, May 2000 as an example.

⁶General Accounting Office, *Chief Information Officers: Implementing Effective CIO Organizations*, GAO-T-AIMD-00-128, 24 March 2000.

H.R. 4670 (Turner), Chief Information Officer of the United States Act of 2000.

- Establishes an Office of Information Technology in the Executive Office of the President to serve as a source of technical, policy, and management analysis, leadership, and advice for the President and federal agencies with respect to the development, application, and management of information technology by the federal government.
- Provides for such office to be headed by a Chief Information Officer who shall be the President's principal adviser on matters relating to such development, application, and management of information technology.
- Establishes in the executive branch a Chief Information Officers Council to assist and advise in the development and implementation of federal policies and practices with regard to agency development, application, and management of information technology.

H.R. 5024 (Davis), Federal Information Policy Act of 2000.

- Establishes an Office of Information Policy in the Executive Office of the President to be headed by a Chief Information Officer (CIO) of the United States who shall be the principal adviser to the President on matters relating to the efficient and effective development, use, and management of information technology and resources by the federal government. Outlines the Officer's duties and grants the Officer certain authorities and duties currently given to the Director of the Office of Management and Budget (OMB) under existing law.
- Incorporates certain provisions of the Government Paperwork Elimination Act concerning the use and acceptance of electronic signatures by executive agencies. Grants the Officer duties under such provisions currently given to the Director.
- Requires the Officer to establish government-wide security and framework policies for the management of programs, and requires such policies to address risk management and assessment. Outlines information security responsibilities of each agency, including the development and implementation of an agency-wide security program for the operations and assets of such agency. Makes each program subject to Officer approval and annual review by agency program officials.

The 2000 Presidential Campaign. During the 2000 Presidential campaign, both major party candidates expressed support for establishing a federal CIO in some form. In a June 2000 policy statement on government reform, then-Governor George W. Bush stated he would designate the Deputy Director of OMB as the federal CIO to coordinate e-government initiatives and facilitate the

development of federal information technology management in general.⁷ Similarly, Vice Presidential candidate Senator Lieberman issued a policy statement in July 2000 indicating his support for a federal CIO or “IT Czar” to work on e-government efforts and coordinate interagency projects.⁸

107th Congress

Since the Bush Administration took office, it has been widely reported that the President still favors the appointment of a federal CIO in some capacity, at the subcabinet level or lower.⁹ In a statement to the Congressional Internet Caucus on March 22, 2001, then-OMB Deputy Director Sean O’Keefe said that the Bush Administration opposed the creation of a separate federal CIO position due in part to concerns about agency accountability. Instead, O’Keefe stated that the Bush Administration intended to recruit a deputy director of management for OMB who will be responsible for oversight of agency-level CIOs and coordinating e-government initiatives.¹⁰

On June 14, 2001 OMB announced the appointment of Mark Forman to a newly created position, the Associate Director for Information Technology and E-Government. As “the leading federal e-government executive,”¹¹ the new Associate Director will be responsible for the e-government fund, direct the activities of the CIO Council, and advise on the appointments of agency CIOs. The Associate Director will also “lead the development and implementation of federal information technology policy.”¹² The new position will report to the Deputy Director of Management at OMB, who in turn will be the federal CIO.¹³

⁷Governor George W. Bush, “Getting Results From Government,” 9 June 2000. [<http://www.georgewbush.com/Media/PDFs/GovtModernizationFactSheetGetResultsfromGov.pdf>]

⁸ Senator Joseph Lieberman, “Lieberman Outlines Revolutionary Potential of E-Government,” 12 July 2000. [<http://www.senate.gov/~lieberman/press/00/07/2000713842.html>]

⁹Patience Wait, “Prospect of Federal CIO Still Lingers in the Wings,” *Washington Technology*, 5 February 2001, p. 1; Diane Frank, “Federal CIO to Head E-gov,” *Federal Computer Week*, 5 March 2001, p.10; Bara Vaida, “Bush Likely to Name Federal CIO, not Technology ‘Czar’,” *Government Executive Magazine*, 11 January 2001, [<http://www.govexec.com/news/index.cfm?mode=report&articleid=19163>]; Carson Carlson, “Bush May Push for ‘Tech Czar’,” *E-Week*, 15 January 2001, p. 1.

¹⁰Drew Clark, “OMB Deputy Says White House Doesn’t Want Federal CIO,” *Government Executive Magazine*, 23 March 2001, [<http://www.govexec.com/dailyfed/0301/032301td.htm>].

¹¹Office of Management and Budget, “Mark Forman Named Associate Director for Information Technology and E-Government,” 14 June 2001, [<http://www.whitehouse.gov/omb/pubpress/2001-13.html>].

¹²*Ibid.*

¹³Diane Frank, “Fed IT Pick Has Deep Résumé,” *Federal Computer Week*, 18 June 2001, p. 10; Shane Harris, “OMB Appoints Technology Czar,” *Government Executive Magazine*, (continued...)

In January 2002, Norman Lorentz began work as the first Chief Technology Officer at OMB. Lorentz, a former USPS CTO, reports to Mark Forman. Lorentz has been tasked to lead and coordinate multiple efforts to identify and develop the *technological architecture* needed to support federal government e-government and other information technology initiatives.¹⁴

Representative Davis (VA, 1st) has indicated he may reintroduce H.R. 5024 in the coming months, perhaps with some revisions to gain wider support, as a means to further the debate.¹⁵ On May 1, 2001 S. 803 (The E-Government Act of 2001) was introduced by Senator Lieberman. This bill was referred to the Governmental Affairs Committee, which held a hearing on the bill on July 11, 2001. Also on July 11, 2001 Representative Turner introduced a companion bill to S. 803, H.R. 2458 (The E-Government Act of 2001).¹⁶ On March 21, 2002, the Governmental Affairs Committee reported S. 803 (now renamed the E-Government Act of 2002) with an amendment. On June 27, 2002, the Senate passed S. 803 unanimously and the bill was sent to the House of Representatives for consideration. A summary of their relevant provisions is listed below, with a more comprehensive overview provided in Appendix B.

H.R. 2458 (Turner), E-Government Act of 2001.

- Establishes an Office of Information Policy in OMB to be headed by a federal Chief Information Officer (CIO). The CIO would provide “overall leadership and direction to the executive branch on information policy,” and serve as the leader and coordinator of federal e-government issues.
- Establishes the CIO Council by law and task it to work with the federal CIO on issues such as developing collaborative multi-agency information technology initiatives, coordinating the development of federal information technology standards, and working with the Office of Personnel and Management (OPM) regarding the recruitment and retention of federal information technology expertise and leadership.
- Establishes a \$200 million-per-year E-Government Fund for interagency information technology projects, administered by the federal CIO.

¹³(...continued)

15 June 2001, [<http://www.govexec.com/dailyfed/0601/061501h1.htm>].

¹⁴Gail Repsher Emery, “OMB Gets First Chief Technology Officer,” *Washington Post*, 11 January 2002, [<http://www.washtech.com/news/govtit/14625-1.html>]; Diane Frank, “Bush Hires First CTO,” *Federal Computer Week*, 11 January 2002, [<http://www.fcw.com/fcw/articles/2002/0107/web-cto-01-11-02.asp>].

¹⁵Karen Robb, “Industry, Lawmakers Revive Call for IT Czar,” *Federal Times*, 4 March 2002, p. 5; Diane Frank, “Fed IT Pick Has Deep Résumé,” *Federal Computer Week*, 18 June 2001, p. 10; William Matthews, “Davis, Council Push for IT Czar,” *Federal Computer Week*, 22 February 2001, [<http://fcw.com/fcw/articles/2001/0219/web-cio-02-22-01.asp>].

¹⁶Tanya N. Ballard, “House Version of E-Government Bill Introduced,” *Government Executive Magazine*, 16 July 2001, [<http://www.govexec.com/dailyfed/0701/071601t1.htm>].

- Establishes a Federal Information Technology Training Center to train federal government personnel in information technology and information resource management skills.
- Establishes an Online National Library through the collaboration of the National Science Foundation, the Smithsonian Institute, the National Park Service, the Institute of Museum and Library Sciences, and the Library of Congress.

S. 803 (Lieberman), E-Government Act of 2002.

- Establishes an Office of Electronic Government in OMB to be headed by an Administrator. The Administrator would provide “overall leadership and direction on electronic government,” and serve as the leader and coordinator of federal e-government issues.
- Establishes the CIO Council by law and task it to work with the Deputy Director of Management of OMB and the Administrator of the Office of Electronic Government on issues such as developing collaborative multi-agency information technology initiatives, developing common performance measures for agency information resources management, and working with the Office of Personnel and Management (OPM) regarding the recruitment and retention of federal information technology expertise and leadership.
- Establishes an E-Government Fund for interagency information technology projects, administered by the Administrator of the General Services Administration.
- Establishes a Federal Information Technology Training Center to train federal government personnel in information technology and information resource management skills.

Issues

A variety of policy options have been proposed, suggesting there is bipartisan support in favor of establishing a federal CIO position. However, there are some dissenting voices raising a number of issues that remain unresolved. This includes whether a federal CIO should in fact be established. If so, the organizational placement of the position, and the scope of responsibility and authority assigned to the position needs to be determined. Some of these issues arise from the implicit paradox of trying to centralize management of decentralized technologies. Others are the result of differing opinions regarding how information technology fits into the general scope of governance.

Should There Be a Single Federal CIO?

Although there is disagreement about the exact nature of the position, support for a federal CIO generated during the closing months of the 106th Congress appears to have grown since the beginning of the 107th Congress. Discussed in greater detail

below, supporters cite a variety of reasons to justify creating a federal CIO position. Some of the reasons include a need to develop government-wide cybersecurity¹⁷ measures and a need for a voice to advocate the appropriate budgetary support for both short and long term information technology projects. Another reason frequently cited is the need to coordinate the growing number of federal e-government initiatives. As more government functions become available online, sustained and focused central leadership becomes critical to improving federal IT performance and enhancing the delivery of services.¹⁸ This includes the development of government information technology standards that will contribute to a robust and secure information infrastructure. A common theme underlying many of these arguments is the belief that the role of information technology in governance requires leadership with strategic vision to ensure that the improved productivity and efficiency expected by the investment in technology is realized. Some observers also point to the role of CIOs in improving the performance and productivity of private sector organizations as an example of what could be done in the public sector.¹⁹

In response, opponents of efforts to establish a federal CIO argue that the responsibilities of such a position are too complex and unwieldy for one person. They believe that it is not possible for an individual to manage and coordinate the various information technology projects and needs across the entire U.S. government. Related to this argument, some critics also contend that centralizing management of government information technology is a step backward rather than forward. Instead, they suggest it is more appropriate to approach IT needs through smaller, interagency groups focusing on a specific task such as the processing of student loan applications online or improving online tax filing procedures.²⁰ Another reason cited by some opponents is the organizational obstacles to change that will not disappear with the establishment of a federal CIO. One obstacle cited is a budget process that favors separate agency projects rather than cross-agency initiatives. Another is a shorter term focus when major IT projects require long term planning and implementation. Some critics are also concerned about the implications for agency-level planning and responsibility. They fear that centralized management by a federal CIO will be a signal to agencies that they can rely on the federal CIO to supplant their responsibility for tougher IT issues and can reduce their resource commitment toward solving them. In contrast, these critics believe that efforts to change from an industrial age

¹⁷See CRS Report RL30153, *Critical Infrastructures: Background and Early Implementation of PDD-63*, by (name redacted), for more information about computer security.

¹⁸General Accounting Office, *Federal Chief Information Officer: Leadership Needed to Confront Serious Challenges and Emerging Issues*, GAO/T-AIMD-00-316, 12 September 2000, p. 2.

¹⁹William Matthews, "A Czar By Any Other Name," *Federal Computer Week*, 5 March 2001, p. 50.

²⁰"Bush Urged Not to Name Federal CIO," *Government Executive Magazine*, 5 February 2001, [<http://www.govexec.com/news/index.cfm?mode=report&articleid=19336>].

government to an information age government must emanate from the bottom-up by agencies rather than from the top-down by a cabinet-level position.²¹

Where Should a Federal CIO be Organizationally Located?

The placement of the federal CIO is perhaps the most hotly contested issue. Specifically, there is disagreement over whether the federal CIO should be placed in the Office of Management and Budget (OMB), or if a new office should be established within the White House to focus solely on information technology issues. In September, 2000 the Subcommittee on Government Management, Information, and Technology of the Government Reform Committee of the House of Representatives held a hearing regarding two bills proposed by Representatives Turner and Davis earlier that summer (discussed above). Much of the testimony focused on the relationship between the proposed federal CIO and the OMB. Then-Deputy Director of Management at the OMB, Sally Katzen, argued that situating oversight of information technology management within OMB's management and budgeting authority was essential for the successful budgeting and execution of information technology programs.

In response, critics of this approach argued that information technology programs are crucial enough to warrant autonomous management and budget authority by specialists who can devote their full energy to the success of government information technology projects. In addition, some observers suggest there are lessons to be learned from the lackluster results of the agency-level CIO provisions in the Clinger-Cohen Act. The GAO has cited the divided attention of agency-level CIOs with multiple spheres of responsibility as an obstacle for implementing information technology management reforms. The GAO has further stated that the role of the CIO is a full-time leadership position requiring complete attention to information resource management issues.²²

The Bush administration has indicated a preference for assigning some of the responsibilities associated with proposals for a federal CIO to the Deputy Director of Management of OMB. The bills introduced by Representatives Davis and Turner during the 106th Congress both called for the creation of a separate position within the White House. It has been reported that Senator Lieberman favors the creation of a new, separate CIO position with deputy director status within the OMB.²³

²¹Patience Wait, "Prospect of Federal CIO Still Lingers in the Wings," *Washington Technology*, 5 February 2001, p. 1; Drew Clark, "OMB Deputy Says White House Doesn't Want Federal CIO," *Government Executive Magazine*, 23 March 2001, [<http://www.govexec.com/dailyfed/0301/032301td.htm>].

²²General Accounting Office, *Chief Information Officers: Ensuring Strong Leadership and an Effective Council*, GAO-T-AIMD-98-22, 27 October 1997. General Accounting Office, *VA Information Technology: Improvements Needed to Implement Legislative Reforms*, GAO/AIMD-98-154, 7 July 1998.

²³William Matthews, "A Czar By Any Other Name," *Federal Computer Week*, 5 March 2001, p. 50.

Potential Responsibilities of a Federal CIO

The responsibilities of the federal CIO are closely related to the organizational location of the position. If the federal CIO is expected to manage interagency projects and influence budget decisions, then the position will need the appropriate authority and stature to successfully carry out the mission of the office. However, there is some disagreement over what that appropriate authority should be. Some proponents, including Representatives Davis and Turner, and many federal agency-level CIOs, favor the idea of the federal CIO being a cabinet-level position. Other policymakers, including President Bush and Senator Lieberman, contend that the federal CIO does not require cabinet-level status.²⁴ On the other hand, in its recent report, “E-Government: The Next American Revolution,” the Council of Excellence favors the creation of multiple positions at both the cabinet and sub-cabinet levels.²⁵

Information Security. More specifically, questions have been raised about oversight of government information security. Some proponents have advocated that the federal CIO should be empowered to develop and implement a comprehensive response to information security threats. Indeed, some observers cite information security as one of the most important roles for a potential federal CIO, noting that federal information security currently falls under the jurisdiction of twelve congressional appropriations subcommittees and in practice is carried out through a multiple of uncoordinated (and potentially incompatible) efforts by various agencies and departments.²⁶

In the September 2000 testimony before the House Government Management, Information and Technology Subcommittee, the GAO made three primary recommendations regarding governmental action to improve the state of federal information security. Two of these three recommendations focused on the centralization of responsibilities. One recommendation was to have greater “prescriptive guidance regarding the level of protection that is appropriate for these systems.”²⁷ The GAO witness observed that discretion is left primarily with the individual agencies to decide which computer security measures to take and how strenuously to enforce them. The second recommendation was to implement “stronger central leadership and coordination of information security-related activities across the government.”²⁸ The GAO witness stated that oversight of government information security was “divided among a number of agencies,

²⁴Ibid.

²⁵The Council for Excellence is a non-profit, non-partisan organization that “works to improve the performance of government at all levels and government’s place in the lives and esteem of American citizens.” [<http://www.excelgov.org>]

²⁶Drew Clark, “Administration Security Expert Touts Benefits of Federal CIO,” *Government Executive Magazine*, 11 December 2000, [<http://www.govexec.com/news/index.cfm?mode=report&articleid=18997>].

²⁷General Accounting Office, *Federal Information Security: Actions Needed to Address Widespread Weakness*, GAO/T-AIMD-00-135, 29 March 2000, p.11.

²⁸Ibid.

including OMB, NIST, the General Services Administration, and the National Security Agency,” and concluded that this dispersed oversight resulted in a lack of “clear and central coordination” over key “roles and responsibilities.” In addition, the GAO witness observed that there was a lack of sharing of information regarding information security vulnerabilities and solutions.²⁹

One of the central arguments in favor of centralized federal information security management is that it will establish a clear level of accountability for federal information security that is currently diffused. However, it is this very concern about accountability that has concerned opponents of this idea. Critics of proposals for an “IT security czar,” argue that agencies will assume they can minimize their responsibility to secure their computer networks. Instead, these critics suggest IT problems such as computer security must be addressed at the agency level where change takes place.³⁰

Budgetary Authority. Another issue is budgetary authority. Many observers consider some control over funding of IT projects critical to the success of a federal CIO. They note that major IT projects require long term planning and implementation that is ill-suited to the short-term focus of most budgetary processes. Currently, interagency projects coordinated by the CIO Council are funded through an ad hoc, voluntary “pass-the-hat” process.³¹

Supporters of proposals to give a federal CIO some budgetary authority argue that having someone who recognizes the financial needs of information technology projects and has control over the flow of funding will help contribute to more stable planning and ensure the completion of the project. There appears to be little if any significant opposition to assigning the federal CIO some form of budget authority. There has also been relatively little debate about what form it would take. Some observers have suggested either having the federal CIO control a portion of the various agencies’ budgets for information technology projects or providing the federal CIO with a single fund to support interagency projects. President Bush appears to favor the latter option. On February 28, 2001, President Bush proposed an “E-Government Fund,” with an initial funding of \$10 million in 2002, which would rise to \$100 million over three years. The fund was to be used by the federal CIO to support interagency e-government projects such as developing a government-wide public key infrastructure (PKI)³² for secure transactions and helping agencies

²⁹Ibid.

³⁰Patience Wait, “Prospect of Federal CIO Still Lingers in the Wings,” *Washington Technology*, 5 February 2001, p. 1; Drew Clark, “House Chairman Opposes Central IT Security Czar,” *Government Executive Magazine*, 30 March 2000, [<http://www.govexec.com/news/index.cfm?mode=report&articleid=11776>]; Drew Clark, “OMB Deputy Says White House Doesn’t Want Federal CIO,” *Government Executive Magazine*, 23 March 2001, [<http://www.govexec.com/dailyfed/0301/032301td.htm>].

³¹Diane Frank, “Bush’s ‘02 Blueprint Pushes E-gov Fund,” *Federal Computer Week*, 5 March 2001, p. 10.

³²See CRS Report RL30836, *Encryption Technology: The Debate in the 105th and 106th Congresses*, by (name redacted), for more information on PKI.

comply with the Government Paperwork Elimination Act (GPEA).³³ However, the fiscal 2002 Post Service appropriations bill that was signed into law on November 21, 2001 provided for only \$5 million for the e-government fund. For the fiscal 2003 budget, President Bush has proposed allocating \$45 million for the E-Government Fund.

Appendix A: Legislation in the 106th Congress

S. 1993 (Thompson), Government Information Security Act

On November 19, 1999, Senators Thompson and Lieberman introduced S. 1993, which was referred to the Committee on Governmental Affairs. It was later reported in the Senate by the committee on April 10, 2000 with an amendment. Although not creating a federal CIO by name, S. 1993 proposed the centralization of federal information security oversight in OMB. The bill specifically assigned these responsibilities to the Director of OMB, who in turn could delegate this authority only to the Deputy Director of Management of OMB. An exception for national security systems was included that allowed these responsibilities to be delegated to the Secretary of Defense and the Director of Central Intelligence. In many respects, the provisions in S. 1993 mirror other proposals calling for the designation of the Deputy Director of Management of OMB as the federal CIO. The bill would have given the OMB the responsibility to establish government-wide information security policies, including the development and implementation of standards and guidelines. In addition, agencies would have been required to conduct independent evaluations annually and report the results to the Director of OMB. These results, in turn, were to be compiled and presented to Congress by the Comptroller General.

H.R. 4670 (Turner), Chief Information Officer Act of the United States of 2000

On June 15, 2000, Representative Turner introduced H.R. 4670, which was referred to the House Committee on Government Reform. The purpose of H.R. 4670 was “to establish a central focal point to provide effective leadership for efforts by the Federal Government to use information technology,” to improve its efficiency and effectiveness, create opportunities for innovation, and to “provide a mechanism for improved coordination among Federal agencies” for the development and management of information technology projects. Among its primary provisions, H.R. 4670 would have established the Office of Information Technology in the Executive Office of the President. This new office was to be headed by the Chief Information Officer of the United States and advise the President on technical policy issues related to “the development, application, and management of information technology by the Federal Government.” The CIO was to be an appointee reporting directly to the President as the principal advisor on information technology matters. The CIO would also be responsible for submitting an annual report to the President and Congress on the progress of information technology initiatives with

³³Diane Frank, “Federal CIO to Head E-gov,” *Federal Computer Week*, 5 March 2001, p. 10.

recommendations for future actions. In addition to appointing the federal CIO as the Chair of the Chief Information Officers Council, H.R. 4670 would have established the CIO Council by law and asked the Council to assist the federal CIO with the coordination of multi-agency initiatives, the development of performance measures, and consult with the private sector to improve federal government information technology practices. The provisions of H.R. 4670 were not applicable to national security systems, as defined by section 5142 of the Clinger-Cohen Act (40 U.S.C. 1452).

H.R. 5024 (Davis), Federal Information Policy Act of 2000

On July 27, 2000, Representative Davis (VA, 1st) introduced H.R. 5024, which was also referred to the House Committee on Government Reform. Similar to H.R. 4670, the purpose of H.R. 5024 was to create opportunities for innovation for the use and management of information technology resources in the federal government, “harmonize existing information resource management laws in order to coordinate and improve the Federal Government’s development, use, and management of information resources,” and “create effective management and oversight of related information security risks including coordination of information security standards.”

H.R. 5024 sought to amend chapters 35-38 of title 44 of the United States Code. The proposed amendments to chapter 35 would have established the Office of Information Policy (OIP) in the Executive Office of the President. It also would have established a federal CIO and deputy CIO to be appointed by the President and confirmed by the Senate. The federal CIO would be the head of OIP and Chair of the CIO Council. The CIO Council would also have been established by law rather than executive order. Under H.R. 5024, the federal CIO was to serve as the principal advisor to the President on information technology matters related to the functions of the federal government. The federal CIO would also have been responsible for providing direction to executive agencies on issues of collection and dissemination of information, public access to public information, statistical activities, privacy, and procurement of information technology. In the area of statistical activities the federal CIO would have been responsible for coordinating the policies and procedures for collection, handling, classification, and sharing of statistical information within and between federal agencies. The federal CIO would also have been empowered to appoint a chief statistician and establish an Interagency Council on Statistical Policy to assist carrying out these duties.

To encourage the use of electronic documents in the federal government, H.R. 5024 would have provided the federal CIO with the responsibility to develop and implement procedures for the use of electronic signatures and to conduct an ongoing study with the National Telecommunications Information Administration (NTIA) on the progress of these efforts. To further support the movement toward electronic documents, H.R. 5024 called for the creation of the Government Information Locator Service (GILS). GILS would have functioned as a distributed agency-based operation to help identify major information holdings, enhance public access, and work towards the development of technical standards to ensure the compatibility of information between agencies. Finally, similar to H.R. 4670, the federal CIO would have been required to submit an annual report to the President and Congress.

The bill proposed amendments to chapter 36 that would have reauthorized a significant portion of the Paperwork Reduction Act (PRA) with few or no changes.³⁴

The bill also proposed amendments to chapter 37 that focused on information security, designating it as specific area of concern for the federal CIO. This chapter of H.R. 5024 would have established an Office of Information Security and Technical Protection (OISTP) within the Office of Information Policy (OIP). The role of OISTP was to serve as the principal advisor of the federal CIO on information security matters (§3703). Overall, this chapter directed the federal CIO to enhance information security measures through a variety of activities including the development of standards and guidelines, sharing best practices, promoting awareness, and making recommendations to the Director of OMB regarding budgetary actions. Although a significant part of the federal CIO's portfolio, §3705 of chapter 37 explicitly holds the individual agencies responsible for actively developing, assessing, and implementing their own information security measures. It also required each agency to conduct an annual independent evaluation of their information security practices and submit the results to the federal CIO.

Proposed amendments to chapter 38 of H.R. 5024 focused on federal CIO's role in general information technology management concerns. Some of the provisions included encouraging performance-based and results-based procurement (§3803), enforcing accountability, developing federal information system standards, and keeping Congress informed of the performance of these efforts (§3802 J). Some observers describe H.R. 5024 as a much more detailed version of H.R. 4670, combined with the primary elements of S.1993 and PRA reauthorization language.³⁵

Appendix B: Legislation in the 107th Congress

H.R. 2458 (Turner), E-Government Act of 2001³⁶

On July 11, 2001, Representative Turner introduced H.R. 2458, a companion bill to the original language of S. 803, which was referred to Committee on Government Reform. H.R. 2458 contains a variety of provisions related to the management and promotion of electronic government services. Its purpose is to establish effective leadership of federal information technology projects, require the use of Internet-based information technology initiatives to reduce costs and increase opportunities for citizen participation in government, and promote interagency collaboration for e-government processes.

³⁴See CRS Report RL30590, *Paperwork Reduction Act Reauthorization and Government Information Management Issues*, by Harold Relyea for a more comprehensive review of PRA.

³⁵Diane Frank, "New IT Czar Bill Introduced," *Federal Computer Week*, 28 July 2000, [<http://www.fcw.com/fcw/articles/2000/0724/web-cio-07-28-00.asp>].

³⁶The language of H.R. 2458 described here is identical to the original language of S. 803 when it was first introduced on May 1, 2001.

Title I establishes new organizational structures and amends different portions of Title 44 of the United States Code. Section 101 would establish the federal CIO position to be appointed by the President and confirmed by the Senate. The Office of Information Policy would be established as an office in OMB. As head of the Office of Information Policy, H.R. 2458 would task the federal CIO with carrying out relevant OMB responsibilities for prescribing guidelines and regulations for agency implementation of the Privacy Act, the Clinger-Cohen Act, information technology acquisition pilot programs, and the Government Paperwork Elimination Act. It would also require the General Services Administration (GSA) to consult with the federal CIO on any efforts by GSA to promote e-government.

Section 103 would amend Title 44 by adding Chapter 36 - Management and Promotion of Electronic Government Services, which focuses on issues related to the functions of the federal CIO, the CIO Council, and the E-Government Fund. This chapter would make the federal CIO responsible for carrying out a variety of information resources management (IRM) functions. Some of these responsibilities would include; reviewing agency budget requests for information technology capital planning and investment, reviewing information technology investment legislative proposals, evaluating the performance and results of agency information technology investments, advising the Director of OMB on IRM resources and strategies, providing “overall leadership and direction to the executive branch on information policy,” promoting the effective and innovative use of information technology by agencies especially through multiagency collaborative projects, administering and distributing funds from the E-Government Fund (discussed in greater detail below), consulting with GSA on the use of the Information Technology Fund to promote e-government projects, serving as the Chair of the CIO Council, establishing and promulgating information technology standards for the federal government, establishing fora for federal, state, local, and tribal collaboration and consultation on information technology best practices and innovation, promoting electronic procurement initiatives, and implementing accessibility standards.

Section 103 would also establish the CIO Council by law, detailing its organizational structure and mandate. In addition, Section 103 would establish a \$200 million-per-year E-Government Fund for interagency information technology projects. The fund would be administered by the federal CIO in consultation with the CIO Council. The provision would also allow funds be made available without fiscal year limitation and require the federal CIO to submit annual reports to the President and Congress regarding the operation of the fund.

Title II focuses on enhancing a variety of e-government services and establishes the federal CIO’s role as the leader and coordinator of federal e-government services. The provisions most directly connected to the responsibilities of the federal CIO are described in greater detail while those less so are described in less detail. Section 201 covers federal agency responsibilities as they relate to the federal CIO. Some of these responsibilities include participation in the CIO Council and submitting annual agency e-government status reports to the federal CIO.

Section 202 would require executive agencies to adopt electronic signature methods that would ensure acceptability and compatibility with OMB standards. Section 203 would direct GSA to develop an online federal telephone directory.

Section 204 would direct the National Science Foundation, the Smithsonian Institute, the National Park Service, the Institute of Museum and Library Sciences, and the Library of Congress to collaborate in the creation of an Online National Library.

Section 205 would direct the federal courts to develop web sites containing information about the operation of the court, dockets, and related materials. Similarly, section 206 would direct regulatory agencies to establish web sites containing relevant public information.

Section 207 would require the federal CIO to conduct a feasibility study on integrating federal information systems across agencies and implement up to five pilot projects integrating data elements. Section 208 would direct the federal CIO to assemble an interagency task force to develop and implement regulations and procedures for the creation of an online database and web site providing access to federal funded research and development data. Section 209 would direct the federal CIO to facilitate the development of common protocols for geographic information systems.

Section 210 would amend the Share-in-Savings procurement provisions of the Clinger-Cohen Act by allowing executive agencies to retain a portion of the savings realized from this type of procurement method. It would also direct the Administrator of GSA to move past the pilot programs and provide general authority to executive agencies to use this procurement method.

Section 211 would direct the Federal Emergency Management Agency (FEMA) to contract with the National Research Council of the National Academy of Sciences to “conduct a study on the use of information technology to enhance crisis response and consequence management of natural and manmade disasters.” It would also direct the federal CIO to conduct pilot projects based on the results of the study.

Section 212 would provide for the establishment of a Federal Information Technology Training Center to train federal government personnel in information technology and information resource management skills. Section 213 would mandate an interagency study on the best practices of federally-funded community technology centers.

Section 214 would direct the federal CIO to contract with a nonprofit, non-partisan organization to examine disparities in Internet access based on demographic characteristics. Section 215 would outline the federal CIO’s responsibilities for maintaining accessibility, usability, and preservation of government information. Among its provisions this section would establish an Advisory Board on Government Information with its members to be appointed by the federal CIO. The board would be tasked to conduct studies and submit recommendations to the federal CIO regarding the development of interoperable cataloguing and indexing standards by federal agencies and ensuring permanent public access to information disseminated by the federal government online.

Section 216 would require the federal CIO to establish a public domain directory of federal government web sites. Section 217 would require the Federal CIO to promulgate community standards for federal web sites regarding features,

operation, and information provided. Section 218 would establish privacy requirements regarding agency use of personally identifiable information and require the federal CIO to establish privacy guidelines for federal web sites. Section 219 would require any of the actions taken under this act to be compliant with section 508 of the Rehabilitation Act of 1973 regarding accessibility to people with disabilities. Section 220 would require the federal CIO to notify Congress if any of the provision in the act were obsolete or counter-productive to its purposes.

Section 301 and 301 authorize appropriations for the bill through fiscal 2006 and has the bill take effect 120 days after it is enacted.

S. 803 (Lieberman), E-Government Act of 2002³⁷

On May 1, 2001, Senator Lieberman introduced S. 803, which was referred to the Governmental Affairs Committee, which held a hearing on the bill on July 11, 2001. On March 21, 2002, the Governmental Affairs Committee reported S. 803 (then renamed the E-Government Act of 2002) with an amendment. S. 803 contains a variety of provisions related to the management and promotion of electronic government services. Their purpose includes to establish effective leadership of federal information technology projects, require the use of Internet-based information technology initiatives to reduce costs and increase opportunities for citizen participation in government, and promote interagency collaboration for e-government processes. The description below reflects the amended version of S. 803, which was passed unanimously by the Senate on June 27, 2002.

Title I establishes new organizational structures and amends different portions of Title 44 of the United States Code. Section 101 would establish the Office of Electronic Government in OMB. This new office would be headed by an Administrator, who would be appointed by the President and confirmed by the Senate. As head of the Office of Electronic Government, S. 803 would task the Administrator with assisting the Director of OMB, and the Deputy Director of Management, in conjunction with the Administrator of the Office of Information and Regulatory Affairs (OIRA) to carry out relevant OMB responsibilities for prescribing guidelines and regulations for agency implementation of the Privacy Act, the Clinger-Cohen Act, information technology acquisition pilot programs, and the Government Paperwork Elimination Act. It would also require the General Services Administration (GSA) to consult with the Administrator of the Office of Electronic Government on any efforts by GSA to promote e-government.

Section 103 would amend Title 44 by adding Chapter 36 - Management and Promotion of Electronic Government Services, which focuses on issues related to the functions of the Administrator of the Office of Electronic Government, the CIO Council, and the E-Government Fund. This chapter would make the Administrator of the Office of Electronic Government responsible for carrying out a variety of information resources management (IRM) functions. Some of these responsibilities would include; advising the Director of OMB on IRM resources and strategies,

³⁷The provisions of S. 803 described here reflects its language as amended on March 21, 2002.

providing “overall leadership and direction on electronic government,” promoting the effective and innovative use of information technology by agencies especially through multiagency collaborative projects, administering and distributing funds from the E-Government Fund (discussed in greater detail below), consulting with GSA “to promote electronic government and the efficient use of information technologies by agencies,” lead activities on behalf of the Deputy Director of Management, who serves as the Chair of the CIO Council, assist the Director “in establishing policies which shall set the framework for information technology standards” to be developed by the National Institute for Standards and Technology,” sponsor an ongoing dialogue with federal, state, local, and tribal leaders to encourage collaboration and enhance consultation on information technology best practices and innovation, promoting electronic procurement initiatives, and implementing accessibility standards.

Section 101 would also establish the CIO Council by law, with the Deputy Director of Management of OMB as chairperson, detailing its organizational structure and mandate. In addition, Section 101 would establish an E-Government Fund for interagency information technology projects. The fund would be administered by the Administrator of the General Service Administration (GSA), with the assistance of the Administrator of the Office of Electronic Government. The provision authorizes appropriations for the E-Government Fund in the following amounts: \$45 million for FY 2003, \$50 million for FY 2004, \$100 million for FY 2005, \$150,000 million for FY 2006, and “such sums as necessary for fiscal year 2007.” The provision would also allow funds be made available until expended and require the Director of OMB to submit annual reports to the President and Congress regarding the operation of the fund.

Section 102 consists of conforming amendments.

Title II focuses on enhancing a variety of e-government services, establishing performance measures, and clarifies OMB’s role as the leader and coordinator of federal e-government services. The provisions most directly connected to the responsibilities of the proposed Office of Electronic Government are described in greater detail while those less so are described in less detail. Section 201 focuses on definitions used. Section 202 covers federal agency responsibilities as they relate to the Director of OMB. Some of these responsibilities include participation in the CIO Council, developing performance measures for e-government initiatives, and submitting annual agency e-government status reports to the Director of OMB.

Section 203 would require executive agencies to adopt electronic signature methods that would ensure acceptability and compatibility with OMB standards.

Section 204 would direct the Director of OMB to work with the Administrator of the General Service Administration (GSA) to “maintain and promote an integrated Internet-based system of providing the public with access to Government information and services.”

Section 205 would direct the federal courts to develop web sites containing information about the operation of the court, dockets, and related materials.

Similarly, section 206 would direct regulatory agencies to establish web sites containing relevant public information.

Section 207 would outline the responsibilities of the Director of OMB for maintaining accessibility, usability, and preservation of government information. Among its provisions this section would establish an Interagency Committee on Government Information with its members drawn from executive branch agencies, the National Archives and Records Administration (NARA), as well as the federal legislative and judicial branches. The Committee would be tasked to conduct studies and submit recommendations to the Director of OMB and Congress regarding the development of interoperable cataloging and indexing standards by federal agencies and ensuring permanent public access to information disseminated by the federal government online.

Section 208 would establish privacy requirements regarding agency use of personally identifiable information and require the Director of OMB to establish privacy guidelines for federal web sites.

Section 209 would provide for the establishment of a Federal Information Technology Training Center to train federal government personnel in information technology and information resource management skills.

Section 210 would direct the Secretary of the Interior, working with the Director of OMB through an interagency working group, to facilitate the development of common protocols for geographic information systems.

Section 211 would amend the Share-in-Savings procurement provisions of the Clinger-Cohen Act by allowing executive agencies to retain a portion of the savings realized from this type of procurement method, and extend the pilot-phase of the program. It would also require the Director of OMB, after the completion of five pilot projects but no later than three years after the effective date of the provision, to submit a report to the Senate Committee on Governmental Affairs and the House Committee on Government Reform regarding the results of the pilot projects.

Section 212 would require the Director of OMB to conduct a feasibility study on integrating federal information systems across agencies and implement up to five pilot projects integrating data elements. Section 213 would mandate an interagency study on the best practices of federally-funded community technology centers.

Section 214 would direct the Federal Emergency Management Agency (FEMA) to contract a study “on using information technology to enhance crisis response and consequence management of natural and manmade disasters.” It would also direct FEMA to conduct pilot projects based on the results of the study.

Section 215 would direct the Director of the National Science Foundation (NSF) to contract with the National Research Council to examine disparities in Internet access based on demographic characteristics. Section 216 would require the Director of OMB to notify Congress if any of the provision in the act were obsolete or counter-productive to its purposes.

Section 301 would repeal the expiration date on the Government Information Security Act (44 USC Sec. 3536).

Section 401 and 402 authorize appropriations for the bill through fiscal 2007 and has the bill take effect 120 days after it is enacted.

Additional Reading

CRS Report RL30153, *Critical Infrastructures: Background and Early Implementation of PDD-63*, by (name redacted).

CRS Report RL30745, *Electronic Government: A Conceptual Overview*, by (name redacted).

CRS Report RL31088, *Electronic Government: Major Proposals and Initiatives*, by (name redacted).

CRS Report RL30661, *Government Information Technology Management: Past and Future Issues (The Clinger-Cohen Act)*, by (name redacted).

CRS Report 98-67 STM, *Internet: An Overview of Key Technology Policy Issues Affecting Its Use and Growth*, by (name redacted), (name redacted), (name redacted), G(name redacted) , and J(name redacted).

CRS Report RL31057, *A Primer on E-Government: Sectors, Stages, Opportunities, and Challenges of Online Governance*, by (name redacted).

EveryCRSReport.com

The Congressional Research Service (CRS) is a federal legislative branch agency, housed inside the Library of Congress, charged with providing the United States Congress non-partisan advice on issues that may come before Congress.

EveryCRSReport.com republishes CRS reports that are available to all Congressional staff. The reports are not classified, and Members of Congress routinely make individual reports available to the public.

Prior to our republication, we redacted names, phone numbers and email addresses of analysts who produced the reports. We also added this page to the report. We have not intentionally made any other changes to any report published on EveryCRSReport.com.

CRS reports, as a work of the United States government, are not subject to copyright protection in the United States. Any CRS report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS report may include copyrighted images or material from a third party, you may need to obtain permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

Information in a CRS report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to members of Congress in connection with CRS' institutional role.

EveryCRSReport.com is not a government website and is not affiliated with CRS. We do not claim copyright on any CRS report we have republished.