

**Statement of Paul Brubaker**  
before the

**Committee on Government Reform**  
**Subcommittee on Technology, Information Policy,**  
**Intergovernmental Relations and the Census**  
**Congressman Adam H. Putnam, Chairman**

on  
**Evolving Role of federal Chief Information Officers**

**July 21, 2004**

Mr. Chairman, Members of the Subcommittee, my name is Paul Brubaker, and I am Executive Vice President and Chief Marketing Officer for SI International, an information technology firm with headquarters in Reston, Virginia.

This afternoon, however, I am testifying on behalf of myself as a former Congressional Staff Member who participated extensively in formulating the Clinger-Cohen Act of 1996 which included information technology-related policies and the establishment of Chief Information Officers. I am also the former Deputy Assistant Secretary of Defense (Deputy Chief Information Officer). I believe that my unique blend of legislative and executive branch experience as it relates to the Clinger-Cohen Act could be helpful in examining the evolution of the Chief Information Officer (CIO) position within the federal government. The statements and views I express today are my own and do not represent the views or opinions of my current employer.

Mr. Chairman, your invitation requested that I address five topics related to the role of the CIO in the federal government. The five topics are:

- 1) What responsibilities of federal CIOs are the most critical to the success of their organization?
- 2) What is the most useful reporting structure for a CIO within a government agency to achieve these responsibilities?
- 3) Is there a specific duration of time in which a CIO must remain in their position to be most effective?
- 4) What characteristics and qualifications should a CIO possess?
- 5) What are the major challenges that CIOs face?

I will address these issues in order.

**What responsibilities of federal CIOs are the most critical to the success of their organization?**

As envisioned under the Clinger-Cohen Act, a federal CIO's most important responsibility is to conduct capital planning and investment control (also known as portfolio management) of their agency's information technology budget. Although there are clearly other responsibilities outlined in the legislation, we felt that the effective management of agency technology investments would enable government agencies to

realize the significant measurable improvements in their mission performance and customer and citizen satisfaction.

We believed that CIOs would act in concert with the Office of Management and Budget (OMB) and their respective agency heads to develop and drive investment guidance in functional areas within their departments. The Act's intent is for CIOs to develop integrated information technology architectures for their departments that would drive investment. Moreover, we envisioned that CIOs and CFOs would work together to fully integrate business and financial systems and to establish systems to track and report on measurable improvements in performance. The legislation encourages CIOs to develop agency-wide guidance that requires individual projects to have sound operational architectures. This would enable the efficient re-engineering of business processes before investing in technology. It also provides a structure for developing sound business cases, ensuring adequate security (i.e., having a security architecture for a project), and conducting risk assessments and risk mitigation plans.

We further intended that CIOs would act as an agency oversight mechanism to work with the functional owners of information technology (IT) systems to ensure that they knew the criteria required before approval of a system investment.

Furthermore, as part of their capital planning and investment control responsibilities, a CIO should be able to come before a Congressional Committee, such as this, outline their agency's top ten investments in information technology, and detail anticipated results of those IT investments in terms of specific measurable performance improvements, qualitative and quantitative.

CIOs' second most important responsibility is providing strategic leadership to the agency management table. CIOs are to work with functional owners within their agencies to help them determine where re-engineering processes and applying technologies can improve network performance and efficiencies.

Additionally, CIOs should spearhead the development and application of best practices from the private sector, other government agencies, and non-profit organizations. Clinger-Cohen encourages CIOs to become advocates for transforming government through the adoption of best practices. As an aside, when I took on an advocate role for best practices during my tenure at the Pentagon, a very senior political appointee within the Defense Department's Comptroller organization told me, "that stuff may work with the private sector, but that isn't how we do business in this building."

It is interesting to note that in the original version of the Information Technology Management Reform Act (ITMRA) of 1995, which served as the basis for the ITMRA version incorporated into Clinger-Cohen, had a requirement for a federal CIO. This original version of ITMRA proposed making the federal CIO position a Presidential Appointment that required Senate Confirmation and reported directly to the head of OMB. This person would have been responsible for assisting all of the departmental and agency CIOs in meeting the requirements of the law. Moreover, the federal CIO was to

ensure that agencies were applying best practices across common functional areas and would have been responsible for approving all high risk programs in excess of \$100 million.

In its current form, the Clinger-Cohen Act clearly states that information resources management is the “primary” responsibility of a federal CIO. The law’s intent is to prevent the CIO from “wearing two hats” – that is holding two positions at the same time. The CIO should be a stand-alone position. In fact, the earlier versions of Clinger-Cohen that we proposed to the Administration officials at the time stated that information resources management (IRM) would be the “exclusive” duty of the CIO, because we did not want CIOs focused on duties outside of their core responsibilities. In the end, we compromised on this point, because it was argued that this language would limit CIOs from being “free to lead the Combined Federal Campaign on behalf of their organization.” Since it seemed reasonable at the time, we regretfully negotiated the exclusivity clause out of the final version of the Act and it became an accepted practice to “dual hat” CIOs.

**What is the most useful reporting structure for a CIO within a government agency to achieve these responsibilities?**

Clinger-Cohen clearly envisions that agency CIOs will report directly to the Agency head. If you carefully examine the law’s structure, the performance accountability rests with the agency head, and the CIO is delegated the responsibility and, presumably, the authority to implement the provisions of the legislation on behalf of the agency head. The Act anticipates that CIOs would have an equal seat at the agency management table as the Chief Financial Officer. In retrospect, it may have been a little naïve to believe that any function within a federal agency would be on the same level as the financial professionals who, based on my experience, hold the power of the purse and consequently have better access to and influence with the agency head.

One major requirement of Clinger-Cohen, which is usually ignored, is for the integration of financial systems with the management systems of government. In particular, Section 5122 of the Act states that the process for conducting capital planning and investment control at an agency “be integrated with the processes for making budget financial and program management decisions within the executive agency.” This is reiterated in the Conference Report language, which in its description of Section 5126, says “The conference agreement includes a provision that would require the head of each agency, in consultation with agency Chief Information Officers and Chief Financial Officers, to ensure the integration of financial and information systems.”

Irrespective of practice, Congress’ intent is clear. The CIOs were to report directly to the agency head, have a seat at the management table, and have visibility and ability to exert oversight and control over the agency’s major technology investments.

**Is there a specific duration of time in which a CIO must remain in their position to be most effective?**

The draft GAO report highlighted the relatively short tenures of most CIOs. This is a critical issue that merits attention. However, I believe that it is an effect of multiple causes. First, political appointees rarely serve longer than the term of the Administration that appointed them. This was the main reason for my departure as Deputy Chief Information Officer of the Department of Defense. Secondly, those coming from outside the government get into office expecting to have a set of responsibilities and authority as outlined in the law and, instead, find that many people within the organization have similar responsibilities and authority, which can reduce their perception of the position's importance. By contrast, I believe that the career CIOs who are more familiar with these government structures manage their expectations accordingly and are much less frustrated by the process. They also understand the agency's political landscape. Consequently, career federal CIOs manage their expectations accordingly and are probably more effective in pursuing their agendas – which may or may not be consistent with Clinger-Cohen's true intent.

Finally, many CIOs find themselves burdened with the responsibility for matters over which they have neither the personnel nor financial resources to effectively manage. One such area is security. Often, when there is an IT-related issue, the CIO is normally tasked with fixing the problem. While it is appropriate for the CIO to issue security policy and create mechanisms to enforce the policy, in most cases they are and should be powerless to fix security IT problems. Again, the Act does not contemplate CIOs as being operators, but rather overseers and thought leaders who add strategic value to their IT operations. And again, it is appropriate for an operational unit or agency charged with the implementation and management of the enterprise infrastructure (and by association security) to report directly to the CIO.

I believe that the additional burdens placed upon CIOs combined with the fact that they are not in the influential positions envisioned by the Act has resulted in many federal CIOs leaving prematurely after relatively short tenures.

Based on my observations since the Act's passage, I now believe that Chief Information Officers' term lengths should be set by law. Specifically, I feel that CIOs should be Presidential appointments with fixed terms that are renewable. These terms should be more than six years, but no more than twelve years. Also, there should be special provisions for retirement prerequisites to entice highly qualified applicants, and these retirement benefits should be contingent upon the completion of their terms. I would further recommend that Section 5125's CIOs should also be subject to Senate confirmation.

## **What characteristics and qualifications should a CIO possess?**

Chief Information Officers in the federal government should have a strong understanding of process improvement, and know how the application of technology can transform organizations' operational effectiveness. As a practical matter, they must be able to develop and enforce standards and criteria that improve the effectiveness of agency technology investments.

A background and familiarity with the concepts of portfolio management, risk management, architecture and process re-design are also critical. This person should be a manager first and a technologist second. This is an important point – CIOs should know about how the technology is applied rather than the mechanics of how the underlying technology works. This role is not about “bits and bytes” – it is about improving the business. CIOs must also balance the position's management requirements with diplomatic skills to develop an effective governance program that includes key functional program areas and their organizations' stakeholders. The CIO's failure to gain consensus and acceptance from the functional areas of the agencies will minimize the CIO's overall effectiveness.

The Clinger-Cohen Act outlined the requirements and background required for both the CIO and Deputy CIO. These two positions should lead any capital planning and investment control activity

The legislation included a specific “Duties and Qualifications” in Section 5125(c).

- (c) DUTIES AND QUALIFICATIONS – The Chief Information Officer of any agency that is listed in section 901(b) of title 31, United States Code, shall –
  - (1) give information resources management duties as that official's primary duty;
  - (2) monitor the performance of information technology programs of the agency, evaluate the performance of those programs on the basis of the applicable performance measurements, and advise the head of the agency regarding whether to continue, modify, or terminate a program or project; and
  - (3) annually, as part of the strategic planning and performance evaluation process required (subject to section 1117 of title 31, United States Code) under section 306 of title 5, United States Code, and sections 1105(a)(29), 1115, 1116, 1117, and 9703 of title 31, United States Code –
    - (A) assess the requirements established for agency personnel regarding knowledge and skill in information resources management and the adequacy of such requirements for facilitating the achievement of the performance goals established for information resources management;

- (B) assess the extent to which the positions and personnel at the executive level of the agency and the positions and personnel at management level of the agency below the executive level meet those requirements;
- (C) in order to rectify any deficiency in meeting those requirements, develop strategies and specific plans for hiring, training, and professional development; and
- (D) report to the head of the agency on the progress made in improving information resources management capability.

The Conference Report additionally states that, “CIOs will possess knowledge of, and practical experience in, information technology management practices of business or government entities.”

Also interesting are the Deputy CIO qualifications as described in the Conference Report, which reflect the priorities where CIO organizations should devote the most attention. Specifically, the Conference Report says that “the conferees intend that the deputy chief information officers...have additional experience in business process analysis, software and information systems development, design and management of information technology architectures, data and telecommunications management at government or business entities.”

I would also promote that one of the most important qualities for the CIO to possess is to be a visionary leader as it relates to the use of technologies within their organization. A well thought-out strategic vision from the CIO, which should be articulated in the agency’s IT strategic plan as required under the Act, should provide the roadmap for all of those in the various functions that use IT to follow. This pronounced vision should ensure that everyone is working together toward the same goal and promotes a collaborative atmosphere.

### **What are the major challenges that CIOs face?**

The CIOs in the federal government face a myriad of challenges. They can all be summed up in one phrase “cultural resistance to change.” The government has some structural management challenges, the first of which is the fact that most departmental organizations reflect Industrial Age management structures and practices, rather than those of the Information Age. It, therefore, is no surprise that we cannot achieve “Information Age” results with an “Industrial Age” bureaucracy. Properly addressing these structural and reporting issues is likely to take a long time.

The GAO report before you, at least in its draft form, mentions the position of Chief Operating Officer, who, as in the private sector, would presumably have the Chief Financial Officer (CFO), CIO, Chief Human Resources Officer (CHRO) and Chief Procurement Officer (CPO) all reporting to this one individual. Based on my two decades of experience working in and with the federal government, I think this is an excellent idea and merits serious consideration. However, I would strongly recommend

that Agency Chief Operating Officers, as well as all CFOs, CIOs, CHROs, and CPOs, be Presidential Appointments that are confirmed by the Senate for periods of more than six, but no more than twelve years. These officers could also be re-appointed once their terms expire, and the terms should be staggered across the agency positions. The bottom line, from my perspective, is that the structure of most federal agencies would benefit enormously from such reforms.

Former Senator William S. Cohen (R-ME), my boss when Clinger-Cohen was passed, was very clear and realistic about his concerns regarding the government's cultural impediments to the Act's success. Just before the Act's enactment date, the Senator said, "(w)e must understand that the statutory changes made by the new law are only half the battle. The other half involves changing the management and organizational culture in agencies, OMB and within Congress. Overcoming cultural barriers will require the commitment of management at the highest levels of the federal government."

Senator Cohen was right, and this culture of resistance to change remains the other half of the battle that we have yet to fully win.

Mr. Chairman and Members of the Subcommittee, I look forward to answering any of your questions.