

**Statement by  
Steven I. Cooper  
Chief Information Officer  
U.S. Department of Homeland Security**

**Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations  
and the Census  
U.S. House of Representatives  
July 21, 2004**

Mr. Chairman and Members of the Subcommittee:

Good afternoon. I am Steve Cooper, Chief Information Officer of the Department of Homeland Security. It is my pleasure to appear before you today to provide my opinion and insights into the role and responsibilities of a Federal Chief Information Officer and the various challenges associated with this position. My views are based upon nearly thirty years as an Information Technology professional, including the past 2 ½ in the federal environment. My experience includes CIO roles in the private sector with Fortune 200 corporations, and senior technical and management roles in information technology consulting to federal, state, local and commercial organizations.

I have served as the CIO of the Department of Homeland Security since its inception. It has been both my pleasure and my privilege to join the ranks of the Federal CIO community. The passage of the Clinger-Cohen Act in 1996 was a bold statement signifying that Information Technology, and the management of this resource, was to be a top priority across the federal government. The creation of the Chief Information Officer position within each department clearly established a leader for the Information Technology function and provided a single focal point for leadership within a federal agency. This measure has been integral in driving an enterprise view of IT investment and capital planning and in promoting more efficient and effective management of IT.

I'd like to offer my thoughts in areas of interest posed by the committee.

We are titled Chief *Information* Officers, not Chief Information *Technology* Officers. I believe strongly that **the primary responsibility of any CIO is to ensure the optimal and appropriate use of information** by a department. Understanding business processes and information requirements is a critical success factor that allows the CIO to serve as the key *information* advisor to senior executives. This understanding, coupled with knowledge of how information technologies may be applied to achieve desired business objectives, place the CIO at the table when policy decisions where IT can make or break a desired objective are being made.

The CIO must also **act as a change agent** by guiding organizational transformation and business process reengineering to most effectively meet the strategic and operational objectives of the

agency. The CIO is one of the few individuals whose view of their agency is always horizontal – the ability to see opportunities for integration, consolidation, and rationalization is imperative for achieving more with less in our resource constrained environment. Of course, continually pushing for change that crosses organizational boundaries usually makes the CIO a target of those who resist change and prefer to protect the status quo, so thick skin helps considerably!

**Leading the use and application of IT assets** deployed across the department, including human and financial resources, is what ensures the ability to use information effectively. This is achieved by effectively **guiding the department’s development and use of Enterprise Architecture** best practices: obtaining senior management and employee buy-in and involvement; demonstrating how IT can enable mission effectiveness and efficiency; guiding the proper choice of technology to meet mission goals; and documenting and using portfolio management techniques to allow rapid decision making regarding IT investment choices in turbulent (i.e., terrorist threatening) times.

I don’t believe there is one answer to the question “how long must a CIO serve to be effective?” The learning curve of a CIO is dependent upon a number of factors, such as the maturity of the organization and the current business environment. In organizations that are more mature and operating in a relatively stable environment, the CIO can likely come up to speed in a year. However, for organizations that are still in the formidable stages of development, the CIO may need to be in place for a longer period of time, in order to understand the business strategy, establish the vision for the IT function, provide direction for IT investments, lead change, and deliver results.

There are several characteristics and qualifications that CIOs should possess. First, a CIO should have **good business skills, a business/mission operations sense**. Effective CIOs must serve the leadership of a Department; we must understand and be able to communicate in business, not technical, language. We have to be able to translate technospeak into business driven communication. Second, we should have **good management skills** to lead an IT organization, to hire, motivate and develop staff, and to operate within a budget. Third, we must be able to **lead change**. We have to understand what motivates people and what matters to them on an organizational and personal level. Fourth, we have a **working knowledge of IT gained from experience**, but do not need to be expert in all IT areas. We need to be able to evaluate the technical competency of key staff and understand recommendations from internal and external technical advisors. Fifth, we must have **great communication skills**, both listening and speaking. They must be marketers and evangelists to promote their products and services. Sixth, they need **a sense of humor**. This job is filled with ups and downs. We’ve got to be able to laugh at ourselves and at the inefficiencies and sources of high frustration that come with the role. Finally, we need Guts. We must be able to place mission first and career second.

A Departmental CIO is held accountable for the entire scope of IT – from IT strategic and capital planning, IT human capital, enterprise architecture, e-government, to information security, including specific statutory responsibility for leading the internal cyber security efforts of the department. These functions touch all areas of the enterprise. The CIO strategically plans for enterprise-wide IT resources and is a critical leader on the organization’s management team. It

is therefore crucial that the CIO be invested with the authority to manage these various aspects of IT.

Organizational placement of the CIO has a direct impact upon that individual's ability to effect the changes necessary to drive the IT function toward success. The CIO must be able to strategically plan for enterprise-wide IT resources and be a critical leader on the organization's management team. This reduces the likelihood that each element within the department will view their IT needs separately, as unique entities, leading to stove-piped IT solutions.

There are additional challenges that all CIOs across the federal government face: lack of direct control of IT spending; balancing the speed for technology refresh with the federal budget cycle; lack of resources – people, funding, time; lack of representation at the business/decision-making tables; communicating IT visions and investment decisions in a manner that is understood by senior management; and maintaining an effective security posture in the face of a constantly changing environment.

While the Clinger-Cohen Act clearly places responsibility for coordination of IT investment decisions with the CIO, there are difficulties in executing this objective if the CIO does not have direct control over IT spending and the IT budgets within a department. Although departmental CIOs have been working for several years to truly align investments strategically and with a view toward what is best for the enterprise, there are still numerous IT projects, and the associated budget dollars, that are hidden inside “programs.” The challenge is to bring together the CIO and Chief Financial Officer communities to work together to eliminate the “burying” of funding, and instead recognize the importance of focusing on IT as a global resource for a department. Hence the structure of DHS forces this interaction on a daily basis.

As mentioned earlier in my statement, it is key that a CIO have good business skills and a business/mission operations sense. These skills are crucial in meeting the challenges associated with communicating with senior management and business leaders. The CIO must communicate, and where necessary educate, the business community on the IT vision and investment decisions.

As technology is changing rapidly, more effective planning for “refreshing” hardware and software must occur. Payoff will come through increased mission performance and lower operating costs. Special incentives to retain, and in some instances to retrain, talented IT professionals; recruiting tools such as bonuses and moving expenses; would allow the CIO to reshape his/her organization rapidly to meet the changing government challenges.

The Federal Information Security Management Act (FISMA) was enacted to further hold leadership accountable for all aspects of information security, and I strongly believe this is the right approach. We should acknowledge that IT security is a huge challenge with a doubling of cyber attacks each year, this has been a fact of life for the past 5 or so years. There are significant difficulties associated with maintaining an effective security posture in large organizations, and FISMA correctly places responsibility for information security squarely on the shoulders of each agency head. This fact, coupled with the additional authorities placed on the CIO, further

strengthens the effectiveness of an enterprise program by ensuring that each organization approaches security from a top-down, corporate perspective.

I thank you again for the opportunity to appear before the committee this afternoon, and I look forward to answering your questions.