

**TESTIMONY OF
Richard A. Spires
Chief Information Officer
U.S. Department of Homeland Security
Before the
House Committee on Oversight and Government Reform
February 27, 2013**

Chairman Issa, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to discuss how the Federal Government invests in information technology (IT) to increase the efficiency and effectiveness of our government. As the Chief Information Officer (CIO) at the Department of Homeland Security (DHS) and Vice Chair of the Federal Government's CIO Council, I plan to speak from real-world experience in addressing the challenges in delivering highly effective IT across the Federal Government.

DHS IT Successes

DHS has made significant strides in IT over the past four years, including improving acquisition oversight, ensuring full consideration of the investment life cycle in cost estimates, establishing procedures to thoroughly vet new requirements and alternative solutions, and adapting full funding policies at appropriate milestones. Our main objectives include rationalizing IT infrastructure, improving program management, leveraging IT across DHS to support more effective mission outcomes, and developing our staff.

Rationalizing Our IT Infrastructure

Driving consolidation, integration, and standardization across IT infrastructure is key to driving significant efficiencies (i.e., cost savings). There are many ancillary benefits to such rationalization as well, including freeing up resources to focus on improving mission effectiveness, such as enabling improved information sharing and service application reuse across Components. DHS recently completed a multi-year wide-area network consolidation to OneNet, which leverages the buying power of the Department for all network services. To do this, we consolidated 16 data centers into two state-of-the-art enterprise data centers. A recent study performed by the DHS Office of the Chief Financial Officer (OCFO) showed that ten of the first completed migrations to enterprise data centers resulted in average savings of 14 percent, which is equal to \$17.4 million in savings annually. As part of the Secretary's Efficiency Review Initiative, we have negotiated more than a dozen enterprise licensing agreements with major software and hardware vendors, resulting in more than \$125 million in cost avoidance or direct savings per year. In Fiscal Year (FY) 2012 alone, the Enterprise Licensing Agreement Program saved DHS \$181 million.

In addition to these efforts, the Department has also rolled out 11 cloud service offerings in areas as diverse as e-mail, mobility, virtual desktops, and basic computing services. Cloud computing's business model is similar to that in the telecommunications and utility sectors and will help the Department reduce its IT capital expenditures, provide transparency into IT spending, and reduce the time to market for new capabilities. Today, DHS is considered a leader in cloud computing and we are helping to drive all of government into implementing cloud computing. Our cloud computing offerings have the ability to drive significant integration along with cost savings. For e-mail, we have migrated 110,000 users to our E-mail-as-a-Service (EaaS) cloud offering. Once fully implemented across the enterprise, we expect to save approximately \$20 million per year. DHS's cloud offerings currently support enhancing DHS's government-to-citizen services, enabling a mobile workforce, reducing capital expenditures, and streamlining time to market for new services in Screening/Vetting, Benefits Administration, and Law Enforcement.

As part of the data center consolidation initiative and establishment of the DHS private cloud services, we established inherited security controls to enhance the security of information systems hosted within a DHS data center. Under the current FISMA Assessment and Authorization process, each system must fully document security controls. This is a duplicative process. At DHS, we had identified a large number of common controls at DHS data centers that systems get as soon as they migrate within our data center. The system security management program only needs to address unique or outlier security controls, drastically reducing the staff cost, technology cost, complexity, and workload. Establishing a similar model for other federal data centers, including cloud computing systems, may yield the same benefits.

Improving Our Program Management

Over the last four years, as DHS CIO, I instituted a rigorous review process of our IT portfolio, with more than 90 in-depth reviews of our own large IT programs, and we have worked with the Components and the acquisition community to develop and implement a number of initiatives to address the most common systemic issues.

First, we have a more robust, tiered governance model to provide more active oversight and governance and to ensure the program has the key executive stakeholders engaged to ensure alignment. While the Department's Acquisition Review Board (ARB) has ultimate oversight responsibility over all large programs, we have added Executive Steering Committees (ESCs) for the highest risk programs. Program ESCs are chartered by the DHS ARB and are responsible for providing more robust oversight and increasing transparency and accountability. For example, the ESC for U.S. Citizenship and Immigration Services (CIS) Transformation is chaired by the CIS Director, meets every two weeks, and has had a positive impact on the outcomes of that program.

Second, we have established Centers of Excellence (COEs) in eight areas to support program management disciplines, to include requirements engineering, cost analysis, and test and evaluation. The COEs work with programs to ensure they are using best practices in these disciplines and can provide guidance and even personnel and training materials to help programs start and stay on track. The COEs also support the TechStat process when we need to address a troubled program.

With this approach, we are working to institutionalize DHS's ability to effectively deliver successful large programs. Improved governance and the use of COEs are beginning to have a positive impact. Over the past two years, the Federal IT Dashboard average rating of all large DHS IT programs has gone from 3.04 to 3.34. To further enhance our governance capabilities and improve transparency across the Planning, Programming, Budgeting, and Execution functions, we have established an enterprise business intelligence capability. To date, we have more than 200 reports that span Finance, IT, Program Health, and Real Property Assets. By the end of FY 2013, we will add integrated reports for people, contracts, and security data, and enable forecasting and simulation capabilities to support out year planning activities.

Leveraging IT across DHS to Support More Effective Mission Outcomes

While we are making progress in integrating IT infrastructure across DHS, there remains potential for synergy across like functions. For instance, every DHS Component performs standard business functions, including human resources and finance. In addition, the Components execute similar functions that support mission outcomes, such as screening, domain awareness, and incident response. For efficiency and effectiveness, we are working to properly integrate, address duplication of, and streamline processes and systems through the use of the DHS Enterprise Architecture (EA) while leveraging existing governance structures.

In its most basic terms, the DHS EA is the roadmap for the implementation of business and technical models to drive improvement in the ways DHS meets its missions and carries out its business. We have divided DHS into 13 different functions (called functional portfolios) that represent both the business (e.g., finance) and those that support the mission (e.g., screening, incident response). Looking at the Department from this perspective enables us to see areas that are natural opportunities for sharing and synergy across DHS.

To augment the work of the EA, we are in the process of establishing portfolio governance boards, in which senior executives from across DHS come together to drive decisions to affect better mission and business outcomes. For instance, much work has been completed in the Information Sharing and Safeguarding portfolio. This function has a "segment" EA (a segment EA is specialized for use at the program or portfolio level) and a strong governance board (Information Sharing and Safeguarding Governance Board, or ISSGB) co-chaired by DHS's Undersecretary for Intelligence and Analysis and CIO. Recently, the Secretary issued the DHS

Strategy for Information Sharing and Safeguarding, which was developed based on the segment EA with the oversight of the ISSGB.

Developing Our Staff

Attracting and developing DHS IT staff is critically important to our long-term success. Over the past two years, we developed the DHS IT Human Capital Strategy, an approach that outlines IT career paths and enables us to more formally address how new workers can progress along a technical or managerial career track. We are currently working to leverage DHS developmental, mentoring, and rotational programs into this strategy. We have a strong mission draw for professionals, and we are partnering with the Office of the Chief Human Capital Officer on how to better market ourselves as a Department, both for IT and cybersecurity professionals.

Challenges

Even with the successes outlined above, recent challenges related to the fiscal environment have put pressure on all IT organizations. There are also evolving and increasing expectations from mission customers and external stakeholders, particularly as they see ever-advancing consumer capabilities in their personal use of technology. Based on my experience in the private sector and in dealing with CIOs in large commercial organizations, the Government could better manage IT. I see three root causes that are barriers to the objective of having Federal IT on a par with leading private sector firms. My list of root causes:

1. **Standardizing IT infrastructure** – A department with a modern, homogeneous infrastructure could save as much as 30 percent on infrastructure costs, field applications more quickly and less costly, and provide improved IT security. Given the structure of Agency budgets and organizations, it is very difficult for an Agency CIO to have the tools available to drive such standardization.
2. **Developing the skills to run IT programs** –There are several requirements for a successful IT program, including proper alignment of stakeholders, involvement of the customer, requirements analysis, architecture, information assurance, etc. The common denominator for successful program execution, however, is the need for a solid program management office.
3. **Institutionalizing flexibility to implement IT best practices** –Agency leadership's need for speed and agility has far outstripped the procurement and finance models in place in the Federal Government today. For the Federal Government to truly leverage its buying power, it must evolve from traditional timelines for budgeting and procurements to greater agility, which is expected by today's business customers.

Addressing these three issues enables IT organizations to be both fast and flexible. They are the keys to IT success and would be transformational for the Federal Government.

Solutions

Taking each of these root causes in turn, there are a number of steps that could be taken related to better management of the Federal Government's investment in IT.

Root Cause 1: Standardizing IT infrastructure

Effectively using current statutory authorities to bring the work of CIOs under proper oversight will help us to promote standardization. The PortfolioStat process is a good start toward standardizing IT infrastructure and leveraging shared services, but we need continue to leverage PortfolioStat through additional changes. I recommend the following suggestions be examined further:

- 1.1 ***IT Staff Reporting*** – Comprehensively review the model used by the Department of Veteran Affairs where the CIO organizations have been consolidated. Sufficient time has passed since that change was made, which should allow for lessons learned to be gleaned from the VA model, including efficiencies, accountability, performance, innovation, and customer service, and provide the ability to determine its applicability on a broader basis within the Federal Government.
- 1.2 ***IT Acquisition Review (ITAR) Process*** – At DHS, we have had an ITAR process for larger procurements (above \$2.5 million) for a number of years and are looking to extend it to all IT procurements. The ITAR process has been a beneficial tool to review a planned IT acquisition in the early development of a program. Establishing an ITAR-related process that establishes that all procurements that involve IT must be reviewed by the Department or Agency CIO will help ensure that IT procurements meet architecture guidelines, are not duplicative, and are properly staffed.

Root Cause 2: Developing the skills to run IT programs

The Federal Government can make headway in addressing the issue of skills, expertise, and experience by addressing this at the Federal level and leveraging existing artifacts and guides. I recommend:

- 2.1. ***Program Management Center of Excellence (PM COE)*** – Establish a PM COE of detailees from Departments and Agencies, which would take best practices, tools, templates, training courses, etc., and drive Federal-wide capabilities that programs can leverage across Departments and Agencies. This PM COE would also mentor program management staffs and offer help to struggling programs both in obtaining the right talent for their programs and in providing expert aid to programs in areas in which they are struggling. This PM COE would leverage expertise across the

Federal Government by disseminating materials through the Federal CIO Council and providing community of interest forums.

Root Cause 3: Institutionalizing flexibility to implement IT best practices

As with all acquisition programs, the Federal Government would benefit from an approach that leverages the IT buying power of the Federal Government while adopting best practices that will lead to lower risk overall and drive needed performance improvements. Specific steps may include:

- 3.1. ***Federal IT Strategic Sourcing Organization*** – This organization, perhaps housed in GSA but with detailees from Departments and Agencies, could be dedicated to IT strategic sourcing opportunities for government-wide buying of commodity IT hardware, software, and services. Governance of this organization could occur through the Strategic Sourcing Leadership Council.
- 3.2. ***Governance for Commodity IT*** – A governance board for each functional area, consisting of relevant stakeholders, could help to drive decisions about the effective use of IT in each of these commodity areas.
- 3.3. ***Reduce impediments to Innovation*** – While driving efficiency is critically important today, innovation helps drive areas that can dramatically improve mission effectiveness. Agencies should fully embrace the tools they have at hand, to include leveraging of the OMB’s Digital Government Strategy and using prize competitions to reward vendor innovation, to solve Government problems.

Performance Measurement

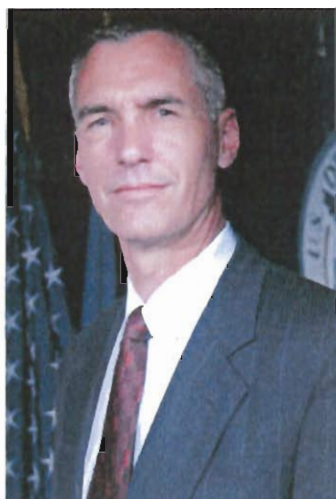
In addition to these recommendations, a mechanism for performance measurement is critical. For each of the three root causes identified above a small number of outcome-based metrics should be defined that will show improved use of IT and serve as a means to measure progress.

Conclusion

Information technology has the ability to meaningfully and measurably improve the mission and business effectiveness of the Federal Government. Thank you for the opportunity to speak with you today and I look forward to your questions.



Richard A. Spires Chief Information Officer



Richard A. Spires was appointed in August 2009 to serve as the Department of Homeland Security's (DHS) Chief Information Officer (CIO). Mr. Spires is responsible for DHS's \$5.6 billion investment in Information Technology (IT). He leads and facilitates portfolio management, development, implementation, and maintenance of the department's IT architecture. Mr. Spires is chair of the DHS CIO Council and the DHS Enterprise Architecture Board. He strongly supports the Secretary's goal of unifying and maturing DHS—establishing one DHS, one enterprise, a shared vision, with integrated results-based operations. Mr. Spires also serves on the Federal CIO Council, where he was selected vice chairman by its members in January 2011. He also serves as co-chair of the Committee for National Security Systems (CNSS). Mr. Spires also previously co-chaired the Federal CIO Council's Federal Data Center Consolidation Task Force and the Management Best Practices Committee.

Mr. Spires held several positions at the Internal Revenue Service (IRS) from 2004 through 2008. He served as the Deputy Commissioner for Operations Support, having overall responsibility for the IRS IT, Human Capital, Finance, Shared Services, Real Estate, and Security functions. Before becoming Deputy Commissioner, Mr. Spires served as the CIO of the IRS, with overall strategic and operational responsibility for a \$2 billion budget and a 7,000-person Modernization and Information Technology Services organization. Mr. Spires also served for two and half years as the Associate CIO for Applications Development and led the IRS Business Systems Modernization program, which is one of the largest and most complex IT modernization efforts undertaken.

From 2000 through 2003, Mr. Spires served as President, Chief Operating Officer, and Director of Mantas, Inc., a software company that provides business intelligence solutions to the financial services industry. In helping to establish Mantas, Mr. Spires successfully led efforts to raise \$29 million in venture funding. Before Mantas, Mr. Spires spent more than 16 years serving in a number of technical and managerial positions at SRA International.

Mr. Spires has been awarded TechAmerica's Government Executive of the Year (2012), Government Computer News's Civilian Government Executive of the Year (2011), and AFCEA Bethesda Chapter's Civilian Government Executive of the Year (2011). He has received two Fed 100 awards (2007 and 2011) as one of the top 100 professionals influencing government IT.

Mr. Spires received a B.S. in Electrical Engineering and a B.A. in Mathematical Sciences from the University of Cincinnati. He also holds a M.S. in Electrical Engineering from the George Washington University. Mr. Spires was named a Distinguished Alumnus of the University of Cincinnati's College of Engineering in 2006.