



TESTIMONY OF  
MR. RICHARD SPIRES  
CHIEF INFORMATION OFFICER  
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE  
U.S. HOUSE OF REPRESENTATIVES  
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM  
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,  
INTERGOVERNMENTAL RELATIONS AND PROCUREMENT REFORM

FEBRUARY 17, 2012

**TESTIMONY OF  
Richard A. Spires  
Chief Information Officer  
U.S. Department of Homeland Security  
Before the  
House Committee on Oversight and Government Reform  
Subcommittee on Technology, Information Policy, Intergovernmental Relations, and  
Procurement Reform  
February 17, 2012**

Chairman Lankford, Ranking Member Connolly, and Members of the Subcommittee, thank you and good morning. Today, I will discuss efforts at the Department of Homeland Security (DHS) to reduce duplicative information technology (IT) investments. As detailed in GAO Public Report, GAO-12-241, *Departments of Defense and Energy Need to Address Potentially Duplicative Investments*, duplicative IT systems exist throughout the Federal Government. By their nature, duplicative IT systems are inefficient; they increase costs, prevent standardization, limit collaboration, and inhibit information sharing among and across the Federal Enterprise. Reducing duplicative IT systems is critical for the efficient operation of our Government, and I am grateful to have the opportunity to testify before you today. I have had the good fortune of being involved in large-scale IT organizations and programs for 25 years in both the public and private sector. Though I see and learn new things in this business every day, the successes and failures I have witnessed throughout my career have helped forge the strong beliefs I hold concerning how to effectively leverage IT to support the mission and business needs of a large organization.

## **Systems Duplication at DHS and in the Federal Government**

The nature of DHS's creation has led to the existence of duplicative systems which we are trying to reduce and consolidate as the Department matures. As the department's architects worked to merge a number of different federal agencies and unite 22 DHS components, legacy systems were patched together to support the five DHS mission areas and address critical business process needs. We stood up DHS very quickly, and, out of necessity, we merged and modified available systems to get the information we needed and the work done.

Looking beyond DHS, there are two main reasons why duplicative systems exist in departments and agencies, and why consolidation of these systems is so difficult. The first reflects a basic human dynamic within organizations. Over time, people seek to optimize their business processes to deliver their specific services or products. These specialized business processes lead organizations to believe they have "unique" requirements that require dedicated, customized solutions to continue meeting needs. Left unchecked, such specialization leads to the creation of unique requirements in even traditional "back office" functions like finance, human resources, and administration.

Beginning in the 1970s, revolutions in technological capabilities led to the development of IT solutions that could standardize and automate mission and business functions. Eager to leverage rapidly modernizing capabilities, government executives developed and deployed IT systems to address their business needs, customizing these systems to meet specific and often unique business needs. However, by the late 1990s, the Federal Government realized that there were significant inefficiencies in allowing each agency to handle IT in this way, and Congress passed

the Clinger-Cohen Act in 1996, followed by the E-Gov Act in 2002. These laws created and were meant to empower an agency Chief Information Officer (CIO) to develop a strong centralized IT capability and to drive efficiencies and effectiveness in providing IT to support agency mission and business needs. The reason duplicative systems remain a decade later is the second reason agencies struggle to eliminate duplication – CIOs and their IT organizations are just one of a number of stakeholders who must concur in order to implement change. The evidence of this is recently documented in a report by GAO entitled, “*Federal Chief Information Officers – Opportunities Exist to Improve Role in Information Technology Management.*” Without an active partnership of CIOs, senior department or agency leaders, and other key stakeholders, the natural inclination of organizations is to drive to unique requirements, making it very difficult to eliminate system duplication.

### **Enterprise and Portfolio Governance Critical to Success**

CIOs are responsible for driving the efficient use of IT in their department or agency. Clearly identifying and eliminating duplicative IT systems is a key component to driving efficiencies in the use of IT. Unfortunately, as CIOs, we cannot just mandate the elimination of these duplicative systems. An effective CIO must find a way to drive the change required to remove duplication in agencies and overcome the desire to maintain the status quo. The key is to develop an environment at the senior executive level that: 1) enables a group of executives representing all appropriate organizations to work collaboratively to understand agency needs in a particular mission or business area; 2) completes a comprehensive analysis in the mission or business area to identify ways to improve both effectiveness and efficiency across the enterprise; and 3) has a decision-making process in which those same executives can effectively drive

change based on the analysis. I have found both in government and the private sector that if you can create these conditions, over time executives will be able to make the hard decisions on the trade-offs and compromises necessary for the good of the enterprise, even if it is not optimal for their own organization. I use the term “strategic alignment” to reflect what is necessary for success. In my experience, the best way to achieve such alignment is through strong enterprise and portfolio governance buttressed by segment enterprise architecture.

Enterprise governance provides large organizations with the ability to effectively make informed decisions that involve stakeholders across the enterprise. The objective is simple: to have key executives across the enterprise determine the optimal allocation of capabilities and resources across programs to best support the achievement of mission and business outcomes. In mature organizations, enterprise governance regularly brings together senior leadership to decide which new capabilities best support the mission and then prioritize them for development and fielding. Effective enterprise governance is integral to the planning cycle before the launch of a new program (or the elimination of an existing system to reduce duplication), providing clear direction and stated outcomes in support of a program’s execution. Mature enterprise governance is focused on all capabilities to produce mission and business outcomes, and, as such, enterprise governance is not specific to just IT or IT programs.

In smaller organizations, it is possible to execute enterprise governance with one governance body that represents top leadership. But, in larger and more complex organizations, it becomes daunting for the top leadership to deal with all programs and program allocation decisions.

Portfolio governance provides the scale necessary for leadership to deal with decisions in large organizations. We break the challenge down into what we call “portfolios,” or logical partitions, that can support various elements of an organization’s mission and business outcomes.

Portfolios may be defined based on the organizational structure of an agency, but, in many instances, the better approach is to have portfolios represent functional groupings that can drive improvements to mission and business effectiveness. The approach to defining a set of portfolios for an organization is unique to that organization’s structure and mission.

For example, DHS has more than 200,000 employees organized into seven large operating components (e.g., U.S. Coast Guard, FEMA, and TSA) along with several other smaller offices and components. A number of these components support similar functions, such as incident response handling (FEMA and the Coast Guard), or the screening of individuals (TSA, CBP, USCIS, ICE, and the Coast Guard). As the DHS Under Secretary for Management has testified, we are implementing a strategy to increase the Department’s effectiveness in fulfilling our missions and business by integrating and aligning functional areas at both the Department and Component levels. In particular, we are working to implement 13 functionally-oriented portfolios to include mission support functions (e.g., securing, screening, and incident response) and business functions (e.g., finance and human resources).

At DHS, it was important that we defined the portfolios functionally to drive cross-component integration since the systems duplication here is a byproduct of our organizational structure. By

defining and analyzing our portfolios along functions, we can more effectively identify and address duplication and redundancy in both business processes and in systems.

In my experience, the most effective model is to create a Portfolio Governance Board for each portfolio. Just like enterprise governance boards, key executives must actively participate in portfolio governance boards. For example, a financial portfolio board would typically be chaired by the CFO as the business executive owner and include an IT executive as a member, along with other executives from closely integrated user communities such as security, procurement, and asset management. Other members of the board may include executives from operating and planning organizations.

### **Segment Enterprise Architecture Leading to Transformation**

So what do these portfolio governance boards do and how can they get it done? Each board looks over a multi-year planning horizon and defines a set of measurable stretch objectives that would significantly improve mission or business effectiveness. Measurable objectives could include items such as reductions in response or service times, customer satisfaction survey scores, or cost efficiencies through elimination of duplicative systems. To achieve those objectives, the portfolio governance board must establish capabilities that are required to meet such objectives. For instance, in a human resource portfolio, a capability may be to have automated end-to-end tracking of all steps in the hiring process, with the objective to reduce the average time to hire by 50%. Once the objectives and capabilities are set, the hard part is defining a goal end state that will meet those objectives for that portfolio. This goal end state

could include business process changes, IT system change, elimination of redundant systems, and other appropriate program changes. To do this work, I recommend the portfolio board be supported by subject matter experts (e.g., finance experts who support the finance governance board) along with the Enterprise Architecture (EA) organization. These specialists, along with EA, provide significant analysis support in defining and analyzing alternatives, along with providing knowledge of the current state. Once a goal state is defined, the board sets a transition strategy that defines the step-by-step process to go from the current, or “as-is,” state to the goal, or “desired,” state. The transition strategy will allocate the capabilities that have been defined to programs for their implementation. If done properly, this transition strategy also serves as the underpinning by which a portfolio governance board can present a cogent budget request that shows how the investments in programs support achieving the goal state.

The approach outlined above applies the generally accepted Federal Segment Architecture Methodology to a portfolio. By applying this methodology and leveraging a robust governance model, we can look across portfolios to identify capabilities and gaps across the enterprise. This is the essence of portfolio governance – to support the strategic goals and objectives of the department or agency and maximize enterprise outcomes while minimizing duplication across systems and investments both within individual portfolios and across portfolios. Portfolio governance also enables a department or agency to identify strategic gaps in mission and business areas and identify the investments required to fill those gaps. The process includes all stakeholders and a governance model to bridge the gap between the “want” and the “need.”

Having implemented such enterprise and portfolio governance in the private sector, the IRS, and now working to mature it at DHS, I know firsthand how difficult this process can be. It takes about three years for a portfolio governance approach to mature to the point where the portfolio has a solid set of business objectives and measures, a defined goal end state, and a viable enterprise transition strategy. This approach cannot be treated as a budget exercise in which you gather people once a year to do analysis. The boards and support organizations must persist, with boards meeting at least every quarter, and typically more often during the first two years upon the standup of a portfolio. Even when mature, the capabilities and end state must be reassessed annually based on changing priorities and realities. The board will then move the planning cycle out by one year, make adjustments to the end-state, and readjust the transition plan. Despite the difficulties, the benefit of this work can be tremendous. It has given me great pride to be associated with organizations that have solid strategies and transition plans. Even in times of significant turbulence, the leadership has sound analysis by which to assess its options and adjust, while still being able to keep its long-term objectives in mind.

### **DHS Example – Human Resources IT Consolidation Drives Transformation**

Recently, DHS reached a milestone in the effort to implement functionally-oriented portfolios for mission-support and business functions: completion of our Human Capital Segment Architecture (HCSA), which will be our model for conducting segment enterprise architectures going forward. HCSA promises to guide real and lasting transformation in our human capital organization.

The HCSA was not an academic exercise but a practical, executable way forward that combines both strategic and tactical approaches. Our first business-driven segment architecture, the HCSA, got underway in November 2010. The project involved a core team of DHS component representatives and enterprise architecture experts from the Office of the CIO working collaboratively with the Chief Human Capital Office (CHCO) planning team to provide project leadership and analysis. Oversight of the HCSA project came from the Human Resources Information Technology Executive Steering Committee (HRIT ESC), a portfolio governance board of human capital and IT executive representatives from every DHS component.

The HCSA effort conducted an in-depth analysis, formulated recommendations for executive review, and ultimately created a plan of action to guide DHS HRIT investments and human capital business processes for the next five years. The plan identifies several near-term efficiencies, as well as critical longer-term improvements to fill automation gaps and reduce redundancy.

Outcomes from this project were not exclusive to technology. The HCSA also took an in-depth look at key business processes that, when combined with enabling technologies, represent the way work is done today. The plan of action cites as many improvement opportunities in business processes as it does in technology. And, for the first time, the vision for human capital is shared across all DHS components. The HRIT Strategic Plan, created as an outcome from this effort, reflects the goals and objectives that will guide the department's HRIT investments over the next five years.

One of HCSA's key outcomes was a first-ever enterprise view of the current state of human capital people, processes, technology, and data. A comprehensive HRIT system inventory revealed 124 HRIT systems at DHS, including many duplicative systems and applications across the enterprise. As an example, DHS currently maintains nine different Learning Management Systems (LMS). The HCSA plan of action will effectively shift a large number of these component-based systems and services to enterprise or Federal Government solutions, reducing redundancy and driving cost savings.

To maintain the momentum of the HCSA effort, we took actions to continue to mature the overall governance process as the HCSA neared completion. The department's HRIT ESC, which reviewed every stage of the HCSA, will continue to make final decisions on HRIT investments and hold components accountable for their role in the transformation. Commitment, accountability, and diligence will be required: from executives to make decisions, from HR and IT subject matter experts to collaborate on transformational projects, and from all organizations to operate within the governance guidelines established and execute on the agreed upon plan of action.

The HCSA has been a watershed for expanding HR and IT communication channels between the department and components. Never before have the department's HR and IT communities worked together so closely for such an extended period of time. The long-term impact of this level of close collaboration on the department's function cannot be overstated. More than 80 DHS employees, including a core team of HR and IT thought leaders from every component,

met regularly to validate analysis, share ideas, and explain their systems, making possible a giant leap forward in aligning and coordinating activity between HR and IT across DHS.

### **DHS Example - Common Operating Picture Technologies Help in Incident Management**

Common Operating Picture (COP) systems are critical for supporting the situational awareness needs of the homeland security mission. Through our portfolio review process, we identified more than 20 different COP investments, most of which were largely uncoordinated, stand-alone investments. To establish governance in this area, we reached out to the National Operation Center (NOC), the DHS component responsible for situation awareness. The NOC has primary responsibility for serving as the nation's homeland security nerve center for information collection and sharing.

DHS now has an effective COP Governance Board chaired by the Director of the NOC. The COP governance board has been operating for about nine months. Under the Director's leadership, all DHS components with COP investments, as well representatives from the DHS Office of Policy, actively participate in activities designed to bring these diverse investments together.

The unity of effort is already producing significant outcomes in the short time the COP governance board has been operating. We have documented more than 1,000 sources of trusted and authoritative data sets used for the homeland security mission. Those engaged in the use of

COP technologies can now rapidly find many key sources of data, enabling them to be more efficient in supporting the mission and avoiding duplication of effort.

As a direct result of the work done by the COP governance board, FEMA provided critical data and technologies to support the NOC during the response to Hurricane Irene. Further supporting the operational mission, the NOC will stand up a new version of the DHS COP later this month. The new DHS COP includes key updates informed by the requirements defined by the COP governance board. The plan is to roll out the new COP to DHS operation centers across the enterprise over the next year, eliminating numerous duplicative COP investments.

In addition to internal coordination, the COP governance board also coordinates with the Federal Geographic Data Committee on the standup of the Federal GeoPlatform. The goal is to assess how this potential shared service can support portions of our unclassified missions and provide solutions for government-to-citizen services. As a result of the efforts of the COP governance board, today we are better able to share information across the department and with homeland security stakeholders more effectively.

## **Conclusion**

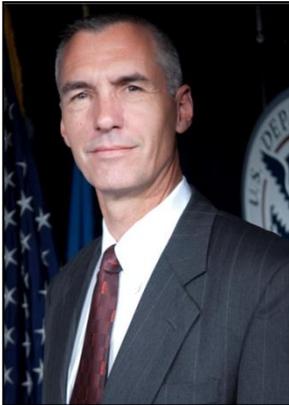
This Administration, under the leadership of Federal Government CIO Steve VanRoekel, recently announced a “Shared First” initiative aimed at rooting out waste and duplication across the Federal IT portfolio. Government agencies must identify and eliminate duplicative IT

systems as part of an overall strategy to enhance efficiencies and drive more effective operations. As I have highlighted, DHS has taken many steps to lead this effort to increase the effectiveness and efficiency of the Department's systems. A collaborative, analysis-based approach that leverages the implementation of robust enterprise governance, cross-enterprise portfolio governance, together with segment enterprise architecture, is imperative to ensuring IT efficiently and effectively supports the mission and business functions of a government agency. A positive byproduct of this work is the identification and eventual elimination of duplicative IT systems. These methods can support implementation of "Shared First," and they should be used throughout the Federal Government to drive real improvements in effectiveness and efficiency in government operations and services.

Thank you.



## **Richard A. Spires** Chief Information Officer



Richard A. Spires was appointed in September 2009 to serve as the Chief Information Officer (CIO) of the Department of Homeland Security (DHS). He is responsible for the department's \$6.8 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 the chairman of the DHS Chief Information Officer Council and the Enterprise Architecture Board.

Mr. Spires 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 council's Federal Data Center Consolidation Task Force and previously co-chaired 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 key support and administrative functions for the IRS, including IT, Human Capital, Finance, Shared Services, Real Estate, and Security functions. Before becoming Deputy Commissioner, Mr. Spires served as 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, being accountable for maintaining more than 400 systems administering in excess of 200 million taxpayer records and supporting more than 100,000 IRS employees. Mr. Spires served for two and half years as the Associate CIO for Applications Development and led the IRS's Business Systems Modernization program, one of the largest and most complex information technology modernization efforts undertaken to date.

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

###