More Security, Less Waste: What Makes Sense for our Federal Cyber Defense

Statement of Former Representative Tom Davis before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

October 28, 2009

Chairman Carper, Ranking Member McCain, I appreciate your efforts to improve information security and am grateful for the opportunity to testify here today.

For 14 years I represented the 11th District of Virginia; I was also honored to serve as a member of the House Committee on Oversight and Government Reform, first as chair of the District of Columbia subcommittee, then as chair of the Technology and Procurement Policy Subcommittee, and finally as chairman and ranking member of the full committee.

My congressional service coincided with the proliferation of the Internet and the explosion of new capabilities that came along, for both the public and private sector. It was clear the revolution in interconnectivity had the potential to fundamentally change governmental operations and service delivery; however, it also created a new form of vulnerability, one in which traditional protections of geographic distance and physical strength were irrelevant. For these reasons, I made information technology, management and security a focus of my work in Congress.

Federal agencies needed to take this threat seriously and ensure proper procedures and tools were in place to protect information systems. Similarly, Congress needed a clear picture of the information security posture of the federal government in order to conduct effective oversight. The Federal Information Security Management Act (FISMA), which I championed in 2001 and 2002, was intended to help provide such a framework.

FISMA requires federal agencies, under the direction of the Office of Management and Budget, to create a comprehensive, risk-based approach to information security management. It further requires annual IT security reviews, reporting and remediation planning at federal agencies. These requirements were based on best

practices and, in addition to safeguarding information, were intended to make security management an integral part of an agency's operations.

At the time FISMA was enacted, no coordinated priority existed to address the threat of cyber attacks. Technology was evolving rapidly. Rather than taking a prescriptive approach, we believed agencies needed to walk before they could run, and putting procedures and protocols in place was an important first step in protecting government's critical infrastructure.

Since its enactment, FISMA has undoubtedly served to elevate the importance of information management and information security in government, and I am proud of the progress the federal government has made through FISMA implementation. That said, there is room for updates and improvement. It is time to take FISMA to the next level.

While I believe the requirements FISMA enumerated would be components of any sound information security plan, the need at present is to "operationalize" its implementation. This would involve tools such as "red team" penetration tests. It would also require appropriate performance measures, such as the time between a penetration and detection; the time to deploy a security patch once it has been released; and the time to complete a root cause analysis when a security breach does occur.

I am pleased your language references both penetration tests and performance measures.

Three other key ingredients: Responsibility, Authority and Accountability.

Chief Information Security Officers (CISOs) may be responsible for overall information security planning, but they cannot just be the bag men when things go wrong. Responsibility for an information security program permeates an organization, from the head of the agency to every employee. Most of the security breaches that have grabbed headlines in recent years aren't the result of some evil cyber genius, but federal employees failing to adhere to basic security protocols. A lost laptop, a stolen Blackberry, computers never returned when an employee leaves an agency – these can result in the personal information of untold thousands being put at risk. CISOs might have to come up with the protocols, but the rank

and file have to adhere to them. As Congress looks at information security issues, it might be wise to consider uniform procedures, training and penalties to reduce theft, loss or other adverse events.

Your language gives CISOs authority to develop, implement and enforce security measures. That's important. There also have to be consequences, good and bad, for failures and successes -- that's one aspect of the accountability component. The private sector provides some models. For example, the payment card industry mandates compliance with standards set by the PCI Security Standards Council. Failure to adhere to these standards results in a business losing the ability to conduct transactions with payment cards. That exact example isn't going to fit the federal system, but we need a system of carrots and sticks that promotes compliance and punishes negligence.

Another aspect of accountability deals with funding. Federal government spending has risen sharply in recent years, but to what end? We have to link performance, in this specific instance performance of information security products and services, with spending decisions. Simply asking for more, or providing more, isn't going to fix the problem, nor is it serving the interests of the American people.

In closing, I would like to reiterate my appreciation for the work you are doing on information security. The Information Age is indeed a strange new world in which a mischievous teenager could be as dangerous as a terrorist organization or malevolent government. I am committed to helping however I can to make sure our federal systems are up to the task and that our oversight mechanisms are commensurate to the need.