TESTIMONY BY

SAMUEL CHUN

DIRECTOR, CYBER SECURITY PRACTICE

EDS U.S. PUBLIC SECTOR,

A HEWLETT – PACKARD COMPANY

BEFORE THE U.S. HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

ON

"THE STATE OF FEDERAL INFORMATION SECURITY"

TUESDAY, MAY 19, 2009

Good morning Chairwoman Watson, Ranking Member Bilbray, and members of the Subcommittee on Government Management, Organization, and Procurement.

On behalf of EDS, an HP Company, thank you for the opportunity to discuss our perspectives on this important topic of federal information security. For nearly 45 years EDS has been a trusted ally, serving governments across the world. As one of the largest providers of technology services and solutions to US federal and state and local governments, we strive daily to achieve secure operational excellence in everything we do.

From the millions of war fighters who carry our identity credentials to the one in five citizens who used our voter registration and election management system last fall , we are entrusted with some of the most sensitive information of our fellow citizens. We understand and appreciate the enormous cyber security challenges that our government agencies face today.

We can attest definitively to the fact that the well-publicized threats facing our information infrastructures are real. Since our founding we have built and managed, on behalf of our government customers, some of the largest and most complex systems and networks in existence. This includes the Navy Marine Corps Intranet (NMCI), the largest purpose-built network in the world. We currently manage 180 data centers, 380,000 servers, 5.4 million desktops and nearly 15 million IP addresses. And we, like everyone else, are constantly under attack. We are also finding the number, type, and sophistication of the attacks to be growing. We expect these trends to continue.

The Federal Information Security Management Act of 2002 was enacted to require federal agencies to improve the security postures of their information systems by implementing a program that would reduce security risks. There is little doubt as to the good intent of FISMA. However, as members of TechAmerica and the Business Software Alliance, we have first-hand knowledge of the debate that rages as to whether FISMA is an effective engine for measuring and improving security performance at agencies. A dispassionate review of FISMA over the last seven years since its enactment yields some tangible benefits that should be acknowledged before we review how FISMA should be reformed to be more effective.

First, it clearly identified (Sec. 3541) that both information security and the role that the private sector plays in it are vital to the national and economic security of the United States. Second, FISMA identified key agencies, specifically NIST and OMB, to set the standards for and oversee security management. By doing so, it provided a government-wide approach that clearly identified processes for inventorying, testing, certifying, accrediting and auditing of systems. This, in turn, provides us, the government integrator community, with a uniform of set of standards and guidelines to follow when implementing systems on behalf of agencies. NIST and its 800 series of special publications are of especially worthy of note as they are relied upon by nearly everyone in the integration community.

While the positive contributions of FISMA are apparent, there is general consensus that FISMA does, in fact, need reform. We've observed and participated in many passionate debates about the effectiveness of FISMA and have concluded that the following deficiencies need to be addressed:

1. Compliance has become too administrative. This is the single most common feedback we hear about FISMA. There is too much emphasis on the generation of paper reports for compliance, certification and accreditation, and auditing. Some have even suggested that it detracts both time and resources away from the real attention required to secure systems. Whether it's by automation or a change in the way reporting is done, action must be taken to reduce the administrative burden of compliance from the agencies.

2. The correlation between compliance and operating performance is unclear. We've observed that some of the most well defended agencies consistently receive poor report cards. In addition, a single grade assigned to a large and diverse agency with many components only generalizes the picture and may not, in fact, provide proper warning of a material vulnerability to mission performance to the agency's mission owners. A more granular approach to reporting that highlights operating performance -- in addition to compliance -- will likely provide more clarity.

3. Accountability for good and poor compliance is unclear. Many have asked what purpose report cards serve other than to paint a broad, general picture of performance for general consumption. While enormous effort is expended in providing these reports and answering audits, it is not transparent how that information is used for the purposes of budgeting, rewards, and assigning accountability. For system integrators, however, there is a clear process for receiving and maintaining the authority to operate through the certification and accreditation process that impact us directly. There should be equally transparent accountability for poor performance. We reiterate our support for the appointment of a new cyber official who can address these concerns.

4. Validity of what is being measured under FISMA is in question. Compliance to FISMA measures how well an agency has accounted for, and applied risk and security management standards, processes, and plans for, information systems. The inference is that as long as the standards, processes and plans are sound, the operational security of an agency is thereby effective. We've observed that much of the debate about FISMA revolves around whether such indirect measures of security required by FISMA compliance adequately ensure operational security performance.

   Direct measures of security performance, such as tracking the number of attacks defended against; the mean time to patch a vulnerability; the number of incidents to which an agency has responded; or the percent of applications tested would provide more rigorous and intensive measures of security. While they provide a much higher level of confidence in the operating performance of a system, they are limited by the sheer scale, size, and scope of the systems being managed in federal agencies. Such real time measures and reporting of agency security performance could enhance both actual security as well as the oversight function. We suggest real rigor and analysis on what combination of measurements will result in the best operating picture of agency so that real insight on the operating picture of an agency is reported.

5. Rapidly emerging threats may be outpacing compliance efforts. Although NIST has been instrumental in setting the standards and processes necessary for industry and

government to conform to, it is unlikely that these standards will keep pace with the rapidly emerging threats. Other organizations such as the US-CERT and the NSA have far greater insight into the emerging threats facing federal agencies. While compliance to standards and processes is essential, we must integrate expertise from other organizations that provide a more real time view into the threats out there in order to be better prepared to meet them in our operations.

Our vision for information security for our customers is simple. Security should be so tightly integrated from the core that agencies have the confidence to be agile at the edge. To put it simply, security should be an embedded part of operations that permeates across the enterprise. Stakeholders should be able to confidently share, receive, and use information with friends and allies without being distracted by concerns of security. By no means, do we think this will be an easy or short journey. In fact we expect this vision will include difficult decisions and foundational changes that will require champions, resources, technologies and definitely the wisdom of time.

That said I think we would be remiss were we not to discuss the first steps and big challenges that must be addressed to take the first positive steps toward our vision.

1. GOVERNANCE: A strong central governance of information infrastructure is vital in defending against cyber threats. Because the threats against information systems and networks can appear without warning, and defense cycle times can be just seconds, lawful orders that change an agency's infrastructure must be carried out quickly and comprehensively throughout the government enterprise. It is not inconceivable that an attack against our government infrastructures could require that rapid changes be made across the entire government enterprise. This highlights the need for clear and consistent roles, responsibilities, policies and accountability structures for the government. Consequently, we strongly support the creation of a new and empowered leader to spearhead this effort.

2. CONSOLIDATION: Consolidating and standardizing infrastructure improves situational awareness, nearly impossible when an agency depends on myriad small, independently operating networks and monitoring systems. Instead, consolidating such networks into fewer, larger tightly controlled operations, such as NMCI, substantially improves security awareness and control. A standardized approach to IT, like the Federal Desktop Core Configuration, substantially improves security by enhancing configuration and change management capabilities as well as baseline security levels. We see substantial benefits in reducing the sheer number and type of networks and infrastructures that operate in agencies.

3. CONSISTENT PROTECTION: Because government infrastructures are vast and interconnected, applying consistent, enterprise wide defense in-depth strategies strongly improves security performance. Recognizing that no single countermeasure is effective against every threat layering of defenses consistently – which includes technologies, processes, and people – mitigates much of the risk. While building layers of defenses to protect systems, networks and the data they carry can be expensive and sometimes impacts user satisfaction, it is a vital strategy in protecting cyberspace. While the urge might be to think of new technologies and tools, we see real need in consistency and enterprise approach as a vulnerability in one area may have potential unintended legacies for everyone.

4. EMPHASIS ON OPERATING PERFORMANCE: While we comply with the various regulatory and audit requirements of our customers, we continue to focus on achieving secure operational excellence by continually reviewing our operating metrics relative to our customer's needs to fulfill their missions. We have recently observed that there has been increased effort during the acquisition process to clearly identify operating performance for security. In particular we've observed enhanced requirements for vulnerability management, incident response, and compliance to standards. We support these efforts to clearly articulate the operating thresholds for security to better meet them.

5. PEOPLE: Lastly we have to focus on our people. Security practitioners clearly must be trained, vetted and industry certified on the best security policies, technologies and practices. This is an area where we have seen substantial progress in industry and government as information security has become a clear and distinct discipline within technology. We need to continue the trend of raising a much larger cyber security workforce.

In summary, we believe secure operational excellence is what we're trying to achieve by reforming FISMA. Security must be more tightly integrated with operations and it will take a conscious effort by operators and users, government and industry alike for embedding security into everything we do -- including technology. For nearly 50 years, EDS has been an ally for governments in tackling some of the most challenging issues that face them. We continue to stand ready to work with you on this one.

Thank you. I'll be happy to answer any questions you might have.