Statement of John Streufert

Chief Information Security Officer /
Deputy Chief Information Officer for Information Security

Bureau of Information Resource Management
United States Department of State

Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security,

Committee on Homeland Security and Governmental Affairs

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

342 Dirksen Senate Office Building
October 29, 2009
2:00 p.m.

Good afternoon Chairman Carper, Ranking Member McCain, and distinguished Members of the Subcommittee:

I am pleased to have this opportunity to testify before the Subcommittee regarding the Department of State's capabilities for securing the Department's global information and technology infrastructure. The Department serves as the "diplomatic front-line" in over 270 overseas posts by serving its 70,000 users with a world-wide network and mission essential software applications. The foreign policy mission makes an inviting target for attack by highly skilled cyber adversaries. However, the Department's layered approach to risk management allows multiple levels of protection. This protection is accomplished by implementing a matrix of technical, operational, and management security controls designed to thwart network threats, detect and mitigate vulnerabilities and strengthen business operations.

In my role as the Chief Information Security Officer, I have become intimately familiar with the benefits, shortcomings and promising opportunities to build upon the current Federal Information Security Management Act of 2002. Our goal is to ensure system security for diplomacy, while continuously improving the return on investment for each dollar spent on cyber security.

The Current Landscape from the Perspective From a Civilian Department

FISMA Benefits. The passage of the Federal Information Security Management Act in 2002 served as a game-changing event for the federal agency community. Whereas, the Health Information Portability and Accountability Act applies to medical information and the Privacy Act of 1974 applies to personal information, FISMA applies to all information used by or on behalf of the federal department and agency. The establishment of a holistic information security program and the responsibility of accounting to oversight entities, including Congress, served as a valuable check in determining the health of an agency's information security program.

Challenges Faced. The federal cyber landscape has changed the past five years. The implementation of federal cyber security has typically been implemented through manual

processes and compliance checks like: (1) conducting an "annual" inventory of systems; (2) testing security controls not less than "annually" , (3) reporting "quarterly" reports of weaknesses to OMB, (4) conducting awareness training "once a year" and (5) performing Certification and Accreditation (C&A) studies every "three" years.

Meanwhile our cyber problems have dramatically escalated in severity and frequency. In a typical week, the Department blocks 3.5 million spam e-mails, intercepts 4,500 viruses and detects over a million external probes to our network. Of that number in the past two years the percentage of malicious code attacks recorded at the State Department in trouble tickets jumped from 38% in the year ending in September 2008 to 79% twelve months later. Comparing monthly totals of trouble tickets for the same two periods, the number of cyber incidents doubled. The volatility of changes to security sensitive settings has been equally problematic.

Ongoing demands for Certification and Accreditations (C&A) studies every three years are the most problematic for our goals. The Department spent $133M over the last six years amassing a total of 50 shelf feet, or 95,000 pages, of final C&A documentation for about 150 major information systems. The electronic working files that support this process over the same period contain 18 Giga-bites of documents with over 33,000 working files. This does not include data bases for tracking system inventory, and tracking Plans of Action and Milestones to resolve pending weaknesses. This equates to cost of the C&A report, which does not include other related products (e.g., system security plans), roughly $1,400 per page. Most compliance driven "snapshots" produce results on paper which are often extraordinarily accurate but out of date within days of being published and are only indirectly connected to the new threats heading toward the Department minute to minute.

Promising Opportunities. In contrast, this month the Office of Management and Budget launched CyberScope, a secure, streamlined, interactive data collection platform for more efficient reporting that also allows research and analysis across Federal agencies.

Additionally, the U.S. Chief Information Officer has formed an interagency task force charged with developing outcome-focused metrics for information security performance by Federal

agencies. Final metrics based on the work of this task force are expected to be released this fiscal year. The National Institute of Standards and Technology (NIST) is revising its current C&A, Special Publication 800-37, by changing the focus of security protection to "continuous monitoring." For its part, the Department began supplementing its FISMA compliance reports and studies with a risk scoring program scanning every computer and server connected to its network not less than every 36 hours on 8 security factors and twice a month for safe configurations of software.

The Risk Scoring Program utilizes best practices such as the Twenty (20) Most Critical Controls also known as the Consensus Audit Guidelines (CAG; a collaborative effort between government and industry), which we have mapped against the way the Department is being attacked. To assess vulnerabilities, the Department utilizes the National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS) from NIST and the Department of Homeland Security where scanning tools tag specific risks with point values from 0 to 10, with 10 being the highest vulnerability... For each risk found, an on-line catalog of security related software flaws offers a help kit for the resolution of that particular vulnerability. When the problem is resolved risk points are deducted and a higher score for the technical team and organizations is computed no matter where they are located across the world.

Since mid-July, overall risk on the Department's key unclassified network measured by the Risk Scoring program has been reduced by nearly 90% in overseas sites and 89% in domestic sites. These methods have allowed one critical piece of the Department's information security program to move from the snapshot in time previously available under FISMA to a program that scans for weaknesses – continuously; identifies weak configurations – each 15 days; recalculates the most important problems to fix in priority order – daily; and issues letter grades (A+ to F) monthly to senior managers tracking progress for their organization the last 30 days.

The various risk score reports tabulate risk scores by region, compare progress overseas to domestic sites, and create an enterprise-wide summary for senior management of the Department. In short, the details empower administrators with targeted, daily attention to conduct remediation and the summaries empower executives to oversee most serious problems.

Conversations I have had with other federal and private chief information security officers encourages me to believe that the State Department experience is both scalable and adaptable to other parts of government and private industry.

Other Elements of Cyber Security Defense in Depth at State

In addition to the Risk Scoring program, the Department's layered approach to risk management includes several other noteworthy initiatives.

Network Monitoring & Incident Response

The Department maintains a 24/7 network watch program that guards against the external penetration, compromise, or misuse of the Department's cyber assets. Analysts stationed at our Network Monitoring Center serve as continuous sentries for inappropriate network activity based on intrusion detection system signatures, reports from the Firewall Team and other sources. The analysts perform preliminary assessments to confirm the nature and source of suspicious network security events. Those matters deemed significant are escalated to the Computer Incident Response Team (CIRT) for in-depth analysis and corrective action.

The CIRT serves as the Department's main clearinghouse for reporting computer security events and incidents occurring on Department and foreign affairs agency networks. CIRT analysts track all reported actions through completion and coordinate incident response actions with all stakeholders including the Department's security units, Department of Homeland Security's US-CERT and law enforcement entities.

Threat Detection

To combat increasingly sophisticated cyber attacks, the Department's Cyber Threat Analysis Program provides overseas posts and Department management with indicators and early warnings about potential cyber incidents. This team of technical analysts performs essential in-depth assessments of network intrusions and helps coordinate the Department's response to sophisticated cyber attacks. They also work closely with the law enforcement and network defense communities to develop both a comprehensive threat picture and possible remediation

measures. In addition, they perform proactive penetration testing and network forensic analysis to detect and resolve significant threat issues.

Global Security Scanning

The Global Security Scanning program of the Department serves multiple essential purposes covering all of its domestic and overseas locations. Electronic tools perform functions that include confirming what is connected to Department networks; assuring that computers, network and software are in the safest configuration of setting, locating system vulnerabilities that need correction and collecting evidence for cyber security investigations. Global scanning is complimented with computer security officers supporting security regionally and locally for overseas posts as "boots on the ground."

Consequences for Cyber Misuse or Abuse

The Department's Cyber Security Incident Program was formed to address consequences for acts of cyber misuse or abuse by individuals. The program enhances the protection of the Department's cyber infrastructure by raising overall cyber security awareness and providing managers with the ability to hold individual users accountable for acts of cyber misuse or abuse. The Department like all parts of the federal government needs to balance the benefits of cyber space for mission effectiveness, with the personal responsibility every employee is asked to demonstrate when using government cyber resources.

The Cyber Security Incident Program applies to all Department system users and defines two different categories of incidents: "infractions", where failure to comply with a specific Department policy exists but does not result in actual damage to the Department's cyber infrastructure and "violations", where failure to comply with a specific Department policy exists and results in damage or significant risk of damage to the Department's cyber infrastructure.

In addition to the types of incidents that lend themselves to detection, the Department's network monitoring and inspections alert key Department officials to risks when they occur. Upon notification of an incident, an investigation is undertaken incorporating several Department

organizations charged with gathering the information necessary to ensure a prompt and appropriate response to the cyber event, while protecting the rights of the accused.

Since the Cyber Security Incident Program was established in 2007 a total of 82 users have been cited for infractions and 14 users have been cited for violations. For those found to have committed an infraction or violation, the consequences available to the Department range from a letter of warning, suspension of network access or further disciplinary action.

Other Federal Activity

The Department of State is involved in multiple government-wide efforts that share its IT security solutions with other Departments and Agencies. The most widely use product is an annual IT security awareness course offered to other federal organizations as a Center of Excellence under the Information System Security Line of Business. So far this offering has been delivered to 33,255 federal employees outside the State Department. The State Department is also active in multiple projects with the inter-agency Committee on National Security Systems working on developing common standards for risk studies and authentication of users on networks.

Mr. Chairman, I want to conclude by emphasizing the Department's policies, technology, business processes, and partnerships in place continue to evolve and meet the continuing challenges of the security threats in the cyberspace environment.

I thank you and the Subcommittee members for this opportunity to speak before you today and would be pleased to respond to any of your questions.