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

Before the
House Committee on Oversight and Government Reform
Subcommittee on Government Management, Organization, and Procurement

Federal Information Security: Current Challenges and Future Policy Considerations

2154 Rayburn House Office Building
March 24, 2010
2:00 p.m.

Good afternoon Chairwoman Watson, Ranking Member Bilbray, 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 over the past five years. The implementation of federal cyber security has typically been implemented through manual processes and compliance checks which have competed with the need to implement Web 2.0 technologies in a secure manner.

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. Since 2008 the number security related tickets has more than doubled, while malicious code attacks increased by 47%. The volatility of changes to security sensitive settings has been equally problematic.

Recent Trends. In October 2009 the Office of Management and Budget launched CyberScope, a secure, data collection platform for reporting that allows research and analysis across Federal agencies. Additionally, the Federal Chief Information Officer has formed an interagency task force charged with developing metrics for information security. The National Institute of Standards and Technology (NIST) has revised C&A Special Publication 800-37 to increase its emphasis on continuous monitoring, including a recommendation for the use of automation to obtain more timely, cost-effective, and efficient monitoring results. The goal is to

give senior leaders better information on the security state of their information systems with which to make risk-based decisions. For its part, in FY 2009 the Department began supplementing 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. To this point, State Department risk scoring program has implemented the sub-set of the 15 Consensus Audit Guideline controls that are susceptible to automated verification.

In the first year of site scoring ending July 2009, overall risk on the Department's key unclassified network measured by the Risk Scoring program was reduced by nearly 90% in overseas sites and 89% in domestic sites. Scores have been relatively stable since then. Notwithstanding this reduction to date, the Department

has decided to make it three times more difficult to achieve the same grades by the end of FY 2010 as part of an ongoing commitment to continuous improvement.

These methods, however limited, have allowed one critical piece of the Department's information security program to move from the snapshot in time previously available under FISMA and its related authorities to a program that scans for weaknesses on servers and personal computers– **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**.** It is the State Department's objective to expand automated verification to as many CAG and NIST 800-53 controls as possible and to all infrastructure and applications as soon as possible, limited only by available resources.

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.

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.

This team of technical analysts performs essential coordinated information sharing as defined in NIST Special Publication 800-61. In addition to the reporting requirements found in this publication, Department of State actively communicates on emerging phishing attack threats realized by the Department of State to help other agencies avoid becoming victims of these same phishing scams. Department of state also utilizes, in partnership with US-CERT, the situational awareness initiative EINSTEIN 2 by analyzing and reporting on events detected through this program.

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.

Moreover, the Cyber Threat Analysis team has developed a strong information sharing capability by routinely briefing other USG agencies on pressing threat data and offering technical assistance and best practices information in an effort to help mitigate risks to federal networks. In addition, they participate in multiple working groups and information sharing organizations designed to enhance coordination among the government's cyber defense teams.

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 14 users have been cited for infractions and 227 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.

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