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

Cybersecurity: Emerging Threats, Vulnerabilities and Challenges

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

2154 Rayburn House Office Building
May 5, 2009
2:00 p.m.

Good afternoon Madam 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 combating cyber threats, detecting and mitigating vulnerabilities, and securing the Department's global information and technology infrastructure. My statement will describe key elements of the Department's information security program.

Madam Chairwoman, as you know from your time at the Department of State, we serve as the "diplomatic front-line" in over 270 overseas posts. This global reach affords the Department a unique perspective on cyber security as we provide for the confidentiality, integrity and availability of a worldwide network, 50,000 users and the systems they use. 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 dual role as the Chief Information Security Officer and Deputy Chief Information Officer for Information Security, I am part of an integrated team. Together technical and operational security experts of the Department work in close coordination to satisfy mission essential requirements ranging from command & control capabilities, network & critical infrastructure protection, law enforcement and intelligence community support. The scope of cyber activity that the Department faces, in a typical week includes blocking 3.5 million spam e-mails, intercepting 4,500 viruses, and detecting over a million external probes to our network.

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 perform essential in-depth assessments of network intrusions and help 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.”

Vulnerability Management

To strengthen its operational capability, the Department created the Risk Scoring Program to help pinpoint and correct the worst network and system vulnerabilities on any particular day and networks world-wide.

Risk points are assigned for cyber threats consistent with vulnerabilities defined in National Institute of Standards and Technology (NIST) guidelines. Every computer and server connected to the State Department network is scanned world-wide on a continual basis. When the risk scoring program began approximately two thirds of the calculated risks including vulnerabilities were found at domestic locations. Total risk points are calculated for each organization each day, and when vulnerabilities are corrected the total risk points are reduced. Based on

progress in reducing vulnerabilities each overseas and headquarters organization is graded from “A” to an “F” for their work during the last month.
Since July 2008, overall risk on the Department’s key unclassified network, measured by the Risk Scoring pilot components, has been reduced by nearly 80% in overseas sites and 55% in domestic sites.

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 to suspension of network access. Select cases resulted in further disciplinary action or referral for criminal prosecution.

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 from 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.

Madam Chairwoman, I want to conclude by reiterating the Department's strategy and programs are continually adapting to match the ever changing threats to cyber security. We believe we have the policies, technology, business processes, and partnerships in place 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.