Statement of
Donald R. Reid
Senior Coordinator for Security Infrastructure
Bureau of Diplomatic Security

House Committee on Homeland Security Subcommittee on
Emerging Threats, Cyber Security, and
Science and Technology

Hearing on Cyber Insecurity:
Hackers are Penetrating Federal Systems and Critical Infrastructures

1539 Longworth House Office Building
April 19, 2007
1:00 p.m.

Good afternoon Chairman Langevin, Congressman McCaul, and distinguished Members of the Subcommittee:

I am Donald R. Reid, the Senior Coordinator for Security Infrastructure, Bureau of Diplomatic Security at the Department of State. I am privileged to have this opportunity to testify before the Subcommittee about a cyber intrusion we experienced at the Department last spring. My statement will concentrate on events surrounding this targeted attack to the State Department's unclassified network in the May to July 2006 timeframe, how and when we detected the intrusion, who we notified and engaged to assist in defending our network, how we mitigated the damage and what improvements we have made at the Department to strengthen our cyber defenses.

Before discussing this intrusion in detail, I would like to inform the Subcommittee generally how the State Department has structured its information technology assets to deal with cyber threats. To meet the Secretary's requirement for the confidentiality, integrity, and availability of IT systems and networks in the conduct of diplomacy, the Chief Information Officer employs a strategic, layered approach to comprehensive risk management of our information and information assets. This security strategy, which we call "Defense in Depth," provides the Department multiple levels of defense and protection through a matrix of operational, technical, and managerial security controls. We focus on identifying and mitigating emerging threats because of our overseas exposure.

At the direction of former Secretary of State Powell, and embraced by Secretary Rice, the Department embarked on an aggressive program to modernize its IT systems and networks ensuring that every employee had Internet access. While Internet access can and has greatly facilitated the conduct of diplomacy, it also brings inherent risks. Our architecture includes requisite perimeter security tools and devices, virus detection and response capability, an effective patch management program, network operations and traffic flow analysis, intrusion detection and response capability, security configuration controls and compliance verification to name a few. Over our unclassified network, we daily process about 750,000 e-mails and instant messages from our more than 40,000 employees and contractors at 100 domestic and 260 overseas locations. Also, on a daily basis, we block 500,000 spam e-mails, intercept 5,100 viruses and detect some 2,000,000 anomalous external probes to our network. At each of our domestic and overseas locations we employ U.S citizen Information System Security Officers. At 10 overseas locations, we also have highly-trained, cyber security engineers.

It is worth noting that the cyber security team at State won the National Security Agency's prestigious Frank B. Rowlett Award for its organizational excellence in information assurance in 2005 – a first for the State Department. Additionally, a number of individual members have won IT community-wide recognition for their contributions and leadership. Now, let me provide you some details about our cyber intrusion last year. In this open session, I will describe how the Department responded as a team with our community of partners to a sophisticated attack, while taking care to avoid those specifics that would make it easier to harm government systems in the future.

In late May 2006, a socially-engineered e-mail was sent to an employee in the East Asia Pacific region. The e-mail appeared to be legitimate and was sent to an actual Department e-mail address. The e-mail contained a Word document attachment of a Congressional speech on a topic germane to this region of the world. Later analysis confirmed the attachment contained exploit code hidden within a known Microsoft application that took advantage of a vulnerability for which there was no readily available patch. Once the recipient clicked on the attachment the embedded malicious code established backdoor communications outside of the Department's network via a Trojan Horse. This external communication was immediately detected by our 24/7 intrusion detection system and the Department's Computer Incident Response Team was activated.

At this point, without full knowledge of how the exploit worked and not wanting to exacerbate the situation, network operations staff was directed to block communications to suspect external IPs and the information system security officer at post was directed to remove the infected devices from the network. In fact, we dispatched an overseas cyber security engineer to the post and began a detailed, on-site analysis of the infected computers. We also reported the malicious activity to US CERT at the Department of Homeland Security.

As we continued tracing the anomalous activity on our network, we identified additional intrusions and compromises both in Washington and other posts in the East Asia Pacific region. Our mitigation activity was continued, and we maintained effective communication with US CERT. As the State Department's cyber analysts tested and evaluated captured malicious code, they shared their results with the greater Computer Network Defense community as well as trusted anti-virus vendors. This real-time information sharing practice resulted in the anti-

virus vendors quickly developing appropriate signatures for detecting and eradicating the malicious code and they deployed their results worldwide through their daily virus definition updates.

Meanwhile, critical analysis by our cyber security engineer at site and our team in D.C. led to the discovery of a previously unknown operating system vulnerability for which no security patch existed. The Department of Homeland Security played a critical coordinating role with Microsoft, urging them to develop and deploy a brand new patch as quickly as possible. State also reached out to the FBI for assistance, leveraging a well-established existing relationship.

At this stage, the CIO directed the establishment of a Task Force; a multi-Bureau working group operating around the clock from within the Secretary's operations center. The Task Force worked with staffs at post in their efforts to mitigate the system compromises, rebuild servers, reset passwords, and performed numerous other related tasks. It should be noted while the intruders' activities greatly concerned us, they did not immediately attempt to steal data. Therefore, Task Force members proposed a set of "tripwires" for disconnecting posts from the Internet if the activity got more daring, especially if data was being stolen. Once the network monitoring staff saw limited data being exfiltrated, Internet connectivity throughout the East Asia Pacific region was immediately severed.

When it became apparent Microsoft was unable to further expedite testing and deployment of a new patch for the previously unknown vulnerability, the Department was left to develop its own interim fix. After consulting with experts in industry and government, the cyber team developed a temporary "wrapper' that would protect systems from being exploited further, but would not "fix" the

vulnerability. The Task Force prescribed a remediation protocol for restoring connectivity for posts that included completely sanitizing infected computers and servers and rebuilding them, changing all passwords, installing several critical patches along with the temporary "wrapper," and updating anti-virus software. These mandatory corrective actions were then confirmed via remote scans from Washington and on-site verification by posts. By early July 2006, all posts were operating normally and we have not experienced similar malicious activity in our unclassified network since. Microsoft did deploy its patch for this exploit in August 2006.

As I know you can appreciate, it is important to our overall success to handle these intrusions quietly and effectively, engaging the minimum number of players needed. We were successful here until a newspaper article telegraphed what we were dealing with. Still, we were able to fully inform the Department's oversight, intelligence and appropriation committees of the significant details of this intrusion while, at the same time, the Department of Homeland Security continued to engage Microsoft to deploy the needed patch.

Mr. Chairman, I want to thank you and the Subcommittee members for this opportunity. I would be pleased to respond to any of your questions.