JAMES R. LANGEVIN
2D DISTRICT, RHODE ISLAND

COMMITTEE ON HOMELAND SECURITY
EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY
CHAIRMAN

BORDER, MARITIME, AND GLOBAL COUNTERTERRORISM

INTELLIGENCE, INFORMATION SHARING, AND TERRORISM RISK ASSESSMENT

HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE
TERRORISM, HUMAN INTELLIGENCE, ANALYSIS AND COUNTERINTELLIGENCE

TECHNICAL AND TACTICAL INTELLIGENCE

Congress of the United States
House of Representatives
Washington, DC 20515–3902

WASHINGTON OFFICE:
109 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225–2735
FAX: (202) 225–5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732–9400
FAX: (401) 737–2982

james.langevin@mail.house.gov
www.house.gov/langevin

The Honorable James R. Langevin
Opening Statement – "Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure"
April 19, 2007

Good afternoon and welcome to the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology hearing on the hacking of federal systems and privately-owned critical infrastructure.

I'd like to begin by thanking the witnesses who appear before us today, and I appreciate your testimony. I'll focus my remarks this afternoon on our first panel, which will discuss the security of information technology on the federal level.

Let me be clear about the threat to our federal systems: I believe the infiltration by foreign nationals of federal government networks is one of the most critical issues confronting our nation. The acquisition of our government's information by outsiders undermines our strength as a nation. If sensitive information is stolen and absorbed by our enemies, we are strategically harmed.

Over time, the theft of critical information from government servers could cost the United States our advantage over our adversaries. This is a most critical issue that we cannot afford to ignore any longer. Today we're hearing from several agencies that have experienced significant cyber attacks against their systems. These are not the only agencies experiencing problems. They are simply the only attacks that have been made public.

In October 2006, hackers operating through Chinese Internet servers launched an attack on the computer system of the Bureau of Industry and Security (BIS) at the Department of Commerce. The hackers penetrated the computers with a "rootkit" program, a form of software that allows attackers to mask their presence and then gain privileged access to the system.

In reviewing the Commerce testimony for today's hearing, I am troubled by several things. Though Commerce first learned on July 13 that its computers were infected, this was not the date of initial infection. In fact, Commerce has no idea how long the attackers were actually inside their systems, nor do they know if the attackers are still within their systems. As far as I can tell from the responses, rogue tunnel audits, authentication changes, and complete machine rebuilds have not occurred. We're also not sure how much information was lost. Though Commerce tells us that data was not "lost," data can easily be "copied" and sent outside through the Internet.

Unfortunately, Commerce isn't the only federal agency with a problem. Prior to the Commerce hack, in June 2006, hackers accessed networks at several State Department locations, including its Washington headquarters, and inside the Bureau of East Asian and Pacific Affairs. They did so by sending a socially-engineered email to an employee. The employee opened the Microsoft Word document attachment, which contained an exploit code.

I am concerned about the temporary fix that State put in place. Security authorities that I have spoken with are highly dubious about the success of "temporary wrappers," the kind which State had to put in place due to the absence of a Microsoft patch for several months. Most targeted attacks involve root-kits, which cannot be detected or stopped by a "temporary wrapper." I don't understand, therefore, why State wouldn't take its entire system offline for a full kernel inspection.

In reading State's testimony, I believe they made the determination that accessibility to data is more important than confidentiality and integrity. If State really valued the latter, they would have taken the system off line and done a full wash. Both agencies insist that these attacks are less serious because they involve "unclassified servers." I disagree.

As you are no doubt aware, FISMA requires federal agencies to track down and identify every device and system on an agency's network, and to make sure that the network topology is fully described. As we learned last week, both State and Commerce received F's in the latest round of FISMA scores. According to page 10 of the Fiscal year 2006 FISMA Report to Congress, the Inspector General at State reported that the agency did not complete at least 50% of its system inventory. The IG at Commerce certifies that at least 96% of Commerce systems have been inventoried.

I will suggest to our panelists today that if they can't certify their network topologies to FISMA, then they can't know for certain that these incidents don't involve the classified networks. Furthermore, just because attacks are occurring on the unclassified network does not mean this isn't sensitive information. Information that may be deemed "classified" in the future may first appear on an unclassified network.

But this isn't just about Commerce and State. I am disappointed and troubled with the Department of Homeland Security's progress in securing cyberspace. The Department is the agency responsible for securing the nation's critical infrastructure, and yet they received a "D" this year on its FISMA score. It is the first time since 2003 that the Department did not receive an "F."

Our issue today is with the NCSD, but I'll be honest with you: I don't know how the Department thinks it's going to lead this nation in securing cyberspace when it can't even secure its own networks. Not only are these grades embarrassing, they're dangerous. Think about all of the critical information the Department is keeping on its networks. I can assure everyone here that the kinds of questions that have been asked to the State Department and the Commerce Department will be asked to DHS.

With regard to NCSD's response to these incidents, I have a few thoughts. It is my understanding that NCSD does not adequately share commonalities of attack information with other agencies that may be at risk. For instance, an agency like Commerce or State that has been hacked by a "zero-day exploit" will provide this information to the NCSD. But the NCSD can't just sit on that information. We need the NCSD to be the group that fuses information from across the federal government together and distributes a product for agencies to use.

Unfortunately, I understand that NCSD does not have protocols in place to share this kind information with other agencies in the federal government or perform that level of work. This subcommittee will continue to monitor these issues to ensure that information sharing and technical response improves.

In closing, I think these incidents have opened a lot of eyes in the halls of Congress. We don't know the scope of our networks. We don't know who's inside our networks. We don't know what information has been stolen. We need to get serious about this threat to our national security.