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 – "Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security"
June 20, 2007

Ladies and gentlemen, good afternoon. I thank the witnesses for appearing before the Subcommittee, and we look forward to your testimony. The Internet has brought our friends close and our enemies closer. As each day passes, another incident reminds us that our information and our IT infrastructures are vulnerable.

- Estonia – a technologically savvy country – was brought to its knees by hackers who took down government websites.

- The Pentagon recently asserted that China is developing viruses to attack computer systems to obtain "electromagnetic dominance early in a conflict."

- The incident formerly classified as Titan Rain suggested that the Chinese have been coordinating attacks against Department of Defense networks for years.

This Subcommittee has been holding a series of hearings on cybersecurity, and it has become clear that the infiltration of federal government networks and the possible theft or exploitation of our information is one of the most critical issues confronting our nation. In April, the Subcommittee discussed a series of attacks perpetrated by hackers operating through Chinese Internet servers against computer systems at the Departments of Commerce and State. Hackers were able to penetrate Federal systems and use "rootkits" – a form of software that allows attackers to mask their presence – to send information back out of our systems. At the time, I was critical of security efforts at both State and Commerce, but assured them that I would be posing the same kinds of questions about network security to DHS. That's why we're here today.

It was a shock and a disappointment to learn that the Department of Homeland Security – the agency charged with being the *lead* in our national cybersecurity – has suffered so many significant security incidents on its networks. DHS reported to the Committee that it experienced 844 "cybersecurity incidents" in fiscal years 2005 and 2006. These incidents occurred on IT networks at DHS headquarters, ICE, CBP, FEMA, and others. I'd like to take a minute to share a few representative incidents:

- A password dumping utility and other malicious files were found on two DHS systems.

- Computers contained suspicious beaconing activity and an IRC bot, which is a generic detection for a group of Backdoor Trojan Horses that allows a hacker to control the compromised computer.

- Workstations infected with multiple Trojans and viruses.

- The User ID and passwords for a local administrator account were found in hard copy.

- A Department website has been compromised.

- Classified emails were sent over unclassified networks.

- A workstation was infected with a Trojan scanning for port 137, an event that clearly demonstrated individuals attempting to scan DHS systems through the internet.

- Unauthorized software was installed on an asset that could allow security-setting circumvention.

- Unauthorized users have been attaching their personal computers to the DHS network

- Unauthorized individuals gained access to DHS equipment and data.

- Firewalls have been misconfigured by a contractor to allow all ICMP traffic to and from the Internet.

- And there have been numerous "Classified data spillages"

I'll stop there. Each of these incidents that I've just mentioned represents a significant security breach. Some of these incidents are the result of blatant disregard of DHS IT policy, and I hope that those responsible have been properly disciplined. But others are reminiscent of classic attack patterns by formidable adversaries – we saw these exact incidents on State Department and Commerce Department computers several months ago.

In spite of the significant vulnerabilities in its systems, the Department doesn't appear to be in any rush to fix them. According to the September 2006 DHS IG report on DHS information systems, 69% of the 3,566 open vulnerabilities that exist on the Department's networks did not include the resources required for remediating those vulnerabilities. In fact, some agencies aren't even reporting incidents to the DHS Computer Security Incident Response Center (CSIRC), as required by law.

These components apparently don't understand that vulnerabilities on their individual systems can affect the entire Homeland Security network. Furthermore, information provided by DHS suggests that the CIO is failing to engage in defensive best practices that would limit penetrations into the DHS networks. DHS does not conduct rogue tunnel audits, ingress/egress filtering on DHS client personal computers, widespread internal and external penetration tests on its systems, audits on IT contractors. DHS hasn't mandated two factor authentication across the Department, which would demonstrate what types of critical vulnerabilities remain on DHS networks. How can DHS be the nation's and the government's cybersecurity leader with this track record?

The fact is, DHS is failing to dedicate adequate funding to network security. The finances show that Mr. Charbo and the Department's leadership continue to under-invest in IT security. Mr. Charbo cut funding for the Chief Information Security Officer and only slightly increased the IT security budget. Experts agree that agencies should allocate around 20% of their IT budgets to cybersecurity, and yet DHS is only spending 6.8% to secure their systems. And all of this is happening while the Department's IT budget was increased by $1 billion last year.

Unfortunately, the failure to invest in defensive measures and mitigate vulnerabilities is jeopardizing the Department's mission. That's the conclusion that the GAO reached in an upcoming report about the IT systems supporting US-VISIT. GAO will report that these IT systems are "riddled with significant information security control weaknesses that place sensitive and personally identifiable information at increased risk of unauthorized disclosure and modification, misuse, and destruction possibly without detection, and place program operations at increased risk of disruption."

What does this mean? It means that terrorists or nation states could be hacking Department of Homeland Security databases, changing or altering their names to allow them access to this country, and we wouldn't even know they were doing it. If we care about protecting our homeland from dangerous people, we have to care about the security of the information that we use to accomplish that mission.

I wish DHS exerted the same level of effort to protect its networks that our adversaries are exerting to penetrate them. But as long as this striking and dangerous imbalance persists, the success of the Department's mission remains in doubt. Again, I thank our witnesses for being here today and look forward to probing these critical issues further.