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

The Honorable James R. Langevin
Statement on the Cyber Initiative
February 28, 2008

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

Statement on the Cyber Intitiative

For years, Federal networks have been under attack. I believe that the infiltration and exploitation of these 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 adversaries, we are strategically harmed.

Last year, as Chairman of the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, I held a series of hearings on the cyber threats to our federal networks and critical infrastructure. It is clear that our failure to secure government networks has more to do with mismanagement, and less to do with inadequate technology. This Administration simply has not made cybersecurity a priority. They have not comprehensively identified or mitigated vulnerabilities on our networks; they have not held anybody accountable for breaches; and they have not invested adequate resources to solve the problems. Unfortunately, we are paying the price today.

I remain deeply concerned about the growing threat to our national critical infrastructure. The effective functioning of many infrastructures is highly dependent on control systems, which are computer-based systems used to monitor and control sensitive processes and physical functions. Cyber attacks against these pieces of infrastructure have the potential to cause serious – if not catastrophic – damage to the economy and our way of life. The Administration's Cyber Initiative does not adequately prioritize this issue.

With the right vision and leadership, we can improve security on our Federal networks and critical infrastructure. There are some promising elements of the Cyber Initiative, but there are also some gaping holes. I assure the American people that we will continue to perform robust oversight on this issue.

Recap of the Subcommittee's Previous Hearings

Last year, as Chairman of the Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, I held a series of hearings on the cyber threats to our federal networks and critical infrastructure. We began in April 2007, with a hearing on cyber attacks against the Departments of State and Commerce. At that time, it was clear to me that the federal government did not understand the severity of the threat. Officials did not know the scope or topology of networks; who infiltrated our networks in the past; who was inside of our networks at the present; and how much information had been stolen. At

that hearing, I promised to begin an investigation to assess the cybersecurity posture at the Department of Homeland Security. Chairman Thompson and I began requesting documents from the Department's Chief Information Officer the following week.

Our second hearing in April focused on the need to reduce critical infrastructure vulnerabilities through investment in research and development. In the last seven years, more than 20 reports from such entities as the INFOSEC Research Council, the National Science Foundation, the National Institute of Justice, the National Security Telecommunications Advisory Committee, the National Research Council and the President's Commission on Critical Infrastructure Protection have all urged the government to do more to drive, discover and deliver new solutions to address cyber vulnerabilities. Yet the Administration routinely proposed reductions or flat funding for research and development efforts at the Department of Homeland Security. Our witnesses described the necessity to dramatically reduce the vulnerability of the national information infrastructure to attack, and make major, strategic investments that can significantly reduce infrastructure vulnerabilities over a five to ten year period.

During a June 2007 Subcommittee hearing, we discussed the preliminary results of our investigation into the security of the Department's networks. Due to poor security practices on its networks, the Department of Homeland Security suffered numerous significant security incidents. Routine security reviews – like rogue tunnel audits, ingress/egress filtering, widespread internal and external penetration tests, and contractor audits – were not performed. Multi-factor authentication was not fully implemented. And in spite of nearly 900 cybersecurity incidents between FY 2005 and FY 2006, the Department continued to under-invest in IT security.

The testimony of the Department's Chief Information Officer, Scott Charbo, was disturbing to the Committee. Although the Chief Information Officer is ultimately responsible for the security of the Department's numerous information networks, Mr. Charbo seemed unaware and unconcerned about any serious malicious activity on the networks he was charged with securing. For example, when asked if he or his security team had requested or received intelligence briefings about Chinese hackers penetrating federal networks, or if Department computers ever exfiltrated information to Chinese servers, Mr. Charbo responded "you don't know what you don't know." This answer was typical of the laissez-faire attitude that he exhibited throughout the investigation, and suggested that neither he nor the rest of the Department was taking the issue of cybersecurity seriously. Chairman Thompson and I sought additional information to determine whether these incidents could be tied to the same attacks that occurred on the networks at State and Commerce.

In September 2007, Chairman Thompson and I concluded that the Department was itself a victim not only of cyber attacks initiated by foreign entities, but of incompetent and possibly illegal activity by the contractor charged with maintaining security on its networks. The Department's intrusion detection systems – designed to monitor networks and issue alerts when outsiders attempted to gain access – were not properly installed and monitored. This resulted in dozens of computers becoming compromised by hackers,

who sent an unknown quantity of information to a Chinese-language web site. We asked the Department's Inspector General to begin an inquiry into these matters and refer the case for criminal investigation.

In October 2007, my Subcommittee again revisited the issue of cybersecurity and critical infrastructure, specifically with regard to the electric grid. The effective functioning of the bulk power system is highly dependent on control systems, which are computer-based systems used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. As such, the cyber risk to these systems is increasing. Intentional and unintentional control system failures on the bulk power system can have a significant and potentially devastating impact on the economy, public health, and national security of the U.S.

The Subcommittee learned about an experimental cyber attack led by DHS researchers at Idaho National Laboratory. This experiment – codenamed Aurora – could inflict significant damage upon the electric sector, and several Members joined me in calling upon the Federal Electric Regulatory Commission (FERC) to investigate whether the owners and operators were implementing mitigations to prevent this attack from occurring. In light of these issues, I joined Chairman Thompson, Chairwoman Jackson-Lee, and Ranking Member McCaul in submitting comments to the FERC rulemaking, arguing that their proposed standards do not sufficiently ensure the production or delivery of power in the event of intentional or unintentional cyber incidents involving critical infrastructures. We suggested adopting standards for control systems proposed by the National Institute of Science and Technology.

Our final hearing focused on the implementation of the cyber aspects of the Sector Specific Plans. These 17 plans – one for each critical infrastructure sector in the U.S. – are supposed to describe how each sector will identify, prioritize, and protect their physical and cyber assets. However, an investigation performed for the Committee by the GAO suggests that many of the 17 plans are incomplete when it comes to cybersecurity. The GAO analyzed the 17 plans under three categories: fully addressed, partially addressed, or not addressed, and found that none of the plans fully addressed all 30 cybersecurity criteria. Even more distressing was the absence of an implementation plan. Because Sector Specific Plans remain a voluntary exercise for all sectors, the Federal government is unable to assess the effectiveness of the private sector's cybersecurity controls.

Each of these hearings suggests that the federal government is vulnerable to a cyber attack against federal networks or critical infrastructure. We must continue to identify vulnerabilities in our systems. We must continue to reduce those vulnerabilities. We must continue to engage the private sector. We must make cybersecurity a priority.