OPENING STATEMENT, AS PREPARED
CHAIRMAN JAMES R. LANGEVIN (D-RI)
SUBCOMMITTEE ON EMERGING THREATS, CYBERSECURITY, AND SCIENCE AND TECHNOLOGY
COMMITTEE ON HOMELAND SECURITY

"CYBERSECURITY RECOMMENDATIONS FOR THE NEXT ADMINISTRATION"
TUESDAY, SEPTEMBER 16, 2008

2:00 P.M. IN 311 CANNON HOUSE OFFICE BUILDING

Good afternoon, and welcome to our final public hearing of the 110th Congress. The Subcommittee on Emerging Threats, Cybersecurity, Science and Technology has tackled a number of critical issues related to our national security, including biological, agricultural, radiological, and nuclear threats. We've had an extremely busy schedule, and I thank all of the Members for their commitment and their leadership over the course of this Congress.

Today we are holding our eighth hearing on cybersecurity. I don't think anyone would disagree when I say that this Subcommittee has established itself as the policy leader in the U.S. Congress on the issue. We've held hearings on hacking incidents at State, Commerce, and DHS; cyber attacks on our Internet infrastructure; oversight of the Cyber Initiative; the need for additional investment in cybersecurity research and development; mitigating cyber vulnerabilities in the electric grid; DHS and critical infrastructure sector plans to mitigate cyber vulnerabilities; and incentives for private sector critical infrastructure owners to mitigate cyber vulnerabilities.

That's a significant number of hearings. But it's one thing to hold hearings, and quite another to improve the security of America. That's our goal, and that's what I want to talk about today.

I believe our oversight has enhanced Federal and critical infrastructure cybersecurity by improving security at DHS, highlighting and filling gaps in Federal cybersecurity policy, and holding individuals in the public and private sectors accountable.

First, we've improved situational awareness and increased security on networks at the Department of Homeland Security and across the Federal government. Our goal on this Committee – one that I've discussed on many occasions – is to make the Department of Homeland Security the gold standard in Federal information security. We've got a long way to go before we get there. But as a result of our investigations and hearings, the CIO's office began receiving more threat briefings. That raises situational awareness. The CIO also began working in a more collaborative fashion with the US-CERT after we questioned why the EINSTEIN system wasn't deployed on more networks at DHS. Shortly after our June 2007 hearing, EINSTEIN was deployed on almost two dozen DHS gateways, providing greater insight into the significant number of attacks on government systems. This helps us know where to commit resources to our defenses.

We saw results from those early Subcommittee hearings. In April 2007, we called for a national-level initiative that would standardize intrusion detection technologies across the Federal government. Eight months later, the Administration announced a new Cyber Initiative to improve the security posture of the Federal government's networks.

Secondly, I believe this Subcommittee's oversight has filled – and will continue to fill – significant gaps that exist in Federal cybersecurity policy. We've spent a significant amount of time on the electric grid, one of our most vulnerable critical infrastructure sectors. In 2007, this subcommittee initiated a review of the Federal government's effort and ability to ensure the security of the bulk power system from cyber attack. We began surveying the Electric Sector to determine their mitigation efforts for the "Aurora" vulnerability. During my review of these efforts, it became evident that mitigation of this vulnerability was highly inconsistent. My colleagues and I were surprised and disturbed to see how dismissive many of these companies were of this

vulnerability, so we began doing all we could to ensure that it would be fixed. Today, because of our hearings, more companies are mitigating Aurora and other cyber vulnerabilities in their systems.

During that review, we also identified inconsistent Federal policies that would leave the grid vulnerable to cyber attack. Last week, I testified before the Energy and Commerce Subcommittee on Energy and Air Quality about the need to provide the Federal Energy Regulatory Commission with emergency authority to ensure the security of the electric system from cyber attack. I am highly optimistic that the Congress will soon consider legislation to grant this authority to FERC, and I thank Chairman Boucher for his initiative on this issue.

Finally, I believe this Subcommittee's oversight has established much needed accountability in both the public and private sectors. For instance, as a result of our investigation into cyber attacks of Chinese origin, the Inspector General, the Office of Security, and the FBI are busy conducting their own reviews of attacks on DHS systems. The contractors responsible for securing these systems also remain under investigation. This would not have happened without the oversight of this Committee, and I hope that the public will soon hear about the findings of these reviews.

After providing misleading or confusing statements to the Committee in May, the North American Electric Reliability Organization has demonstrated a new commitment to cybersecurity, and they should be commended for their efforts thus far. After our hearing, NERC announced a process to create new standards for cybersecurity and created a new position of Chief Security Officer for the electric grid. I was glad to see NERC endorse the FERC emergency authority legislation last week, and look forward to watching their continued progress on this issue.

I want to take this opportunity to thank my partner and Ranking Member Michael McCaul, who has been a true ally in this effort. We've done some good work so far, but there is much work ahead of us. That is why we are here today.

In October 2007, Mike and I were named co-chairs of the Center for Strategic and International Studies' Commission on Cybersecurity for the 44th Presidency. The CSIS Commission is a non-partisan commission composed of approximately 30 renowned cybersecurity experts, both in and out of government, from across the country. It is an impressive, experienced, and diverse group of people, and we are glad to be joined by three Members of the Commission – Jim Lewis, the program director; Harry Raduege, one of our co-chairs; and Paul Kurtz, a member. Unfortunately, Scott Charney, Vice President of Trustworthy Computing at Microsoft, and the other co-chair of the group, was unable to attend today, but he has been vital to the Commission's work and I want to acknowledge his contributions and leadership.

We are here to talk about what the next Administration needs to do to improve cybersecurity. There are a number of significant issues that the incoming Administration will face: new organization and national strategies must be considered; legal authorities altered and enhanced; investment and acquisition policies shaped; regulation and incentive regimes revised; and government relationships with the private sector restored.

Congress plays a key role in the future of cybersecurity policy. Just as this Administration hasn't spoken with one voice, however, committee jurisdictional squabbles threaten to divide the attention and focus of Congress on these issues. That is why I'm announcing today that Mike and I have created the first House Cybersecurity Caucus. The purpose of this Caucus is to raise awareness and provide a forum for Members representing different committees of jurisdiction to discuss the challenges in securing cyberspace. We've already received great support from a number of Members, and we look forward to having our kick-off event in January 2009.

Thank you to my fellow Members on the Subcommittee for their participation, and thanks to the witnesses for their appearance today.