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

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

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

The Honorable James R. Langevin

Opening Statement – Joint Hearing: "Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans"
October 31, 2007

Good afternoon. Over the past few months, the Subcommittee on Emerging Threats, Cybersecurity and Science and Technology has held numerous hearings to assess how far reaching our cybersecurity vulnerabilities are and how best to address them. Today we will be focusing on the extent to which cybersecurity has been implemented as part of our 17 different Sector Specific Plans. We are joined today by the Transportation Security and Infrastructure Protection Subcommittee, led by Chairwoman Jackson-Lee and Ranking Member Lungren. Though this is our first joint hearing on the subject, I very much look forward to working with the Chairwoman and Ranking Member on these issues as the 110th Congress continues.

Although critical infrastructure protection is usually associated with physical protection of facilities, there is a growing realization that cybersecurity must receive equal attention. This holds true especially since the nation's critical infrastructure relies extensively on computerized information systems and electronic data. As we learned two weeks ago in a hearing on control systems and the electricity grid, many elements of our nation's critical infrastructure are vulnerable to cyber attack in part because their computers are connected to the Internet. A cyber attack against a portion of our critical infrastructure could have devastating consequences that cascade across the country. Similarly, an attack on our control systems could cause serious physical harm, for example through the introduction of raw sewage into drinking water systems or through the catastrophic failure of critical electrical generators.

One of the most important ways we can secure our infrastructure is through the implementation 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. These Plans are based on the high level Federal guidance in the the National Infrastructure Protection Plan – or NIPP – released by DHS in 2006. The NIPP is the road map for the sectors to follow when developing their Sector Specific Plans. The completion of the Sector Specific Plans will allow DHS to write a National Annual Report on Critical Infrastructure Protection, which is designed to give us a general assessment of the security of our infrastructure. The first annual report is scheduled to be released next week.

Today we will focus specifically on the cyber aspects of these plans. I have two significant concerns about the efforts of the Department of Homeland Security. First, according to the Government Accountability Office report released today, many of the 17 plans are incomplete when it comes to cybersecurity. The GAO rated the 17 Sector Specific Plans according to three categories: fully addressed, partially addressed, or not addressed, and found that none of the plans fully addressed all 30 cybersecurity criteria. GAO reports that many plans have no way of identifying the consequences of a cyber attack or reporting metrics of progress in implementing the plans to DHS. GAO concluded that

without comprehensive plans, certain sectors could be ill prepared to properly respond to a cyber attack.

Now, the plans are supposed to be the easier part of this process. But if we're struggling just to get the plans right, we're going to have an even tougher time achieving true security. Our main goal, of course, is actually protecting our critical infrastructure, or at least making it resilient to attack. That should be the primary focus of our efforts, but, as a first step, DHS must improve the current state of the cyber elements of the sector specific plans. What we have now is simply unacceptable. My second concern is with the implementation of the plans. Today's sector witnesses will describe the varying degrees to which they have begun translating their plans into actual improvements. It should be noted that the sector plans were officially released in May 2007, so there has not been a great deal of time for action. While many sectors have started implementing their plans, much work remains to be done. Under the Department's current public/private partnership approach, I do not believe the Federal government can adequately ensure the security of our critical infrastructure.

Thus far, DHS has adopted a laissez-faire approach toward critical infrastructure owners and operators. The Sector Specific Plan process is entirely voluntary, and there are no regulatory requirements attached to it. Many would argue, however, that protecting critical infrastructure is an issue of national security, a core constitutional responsibility of the Federal government. Under this viewpoint, laissez-faire is arguably not the appropriate model. This observation is not intended to be an argument for more regulation or a criticism of our private sector partners. In a perfect world, we either wouldn't have to worry about security or would have an unlimited amount of money to spend on it. But this is clearly not a perfect world.

The Federal government and the American people want to ensure there is a high level of cybersecurity protections on our critical infrastructure, but, as Dr. Gordon notes in his testimony, private sector owners and operators have a hard time "making the business case" for increased cybersecurity investments. Recognizing that there may in fact be a market failure when it comes to private sector cybersecurity, I've asked the second panel witnesses to discuss ways to incentivize owners and operators of critical infrastructure to better protect their systems. Some believe that with the proper incentives, the private sector can respond faster and more efficiently to future threats. Clearly, without appropriate consideration of all available public policy tools, the private sector's participation in critical infrastructure protection efforts may not reach its full potential.

I have great apprehension about the current framework DHS is creating with the sector specific plans as they relate to cybersecurity. But I am hopeful that today's discussion will be a valuable tool in trying to strike the right balance that will ensure a high level of security with a low level of government involvement.