**Statement of Rep. James R. Langevin**
**Ranking Member on House Armed Services Subcommittee on**
**Emerging Threats and Capabilities**

**Hearing Before the Senate Committee on Judiciary**
**Subcommittee on Crime and Terrorism**

**June 21, 2011**

I would like to thank Chairman Whitehouse and Ranking Member Kyl for inviting me to testify before the Judiciary Subcommittee on Crime and Terrorism on one of the most critical national security challenges facing our country today, and the Administration's proposal to address this threat. Cyber incidents have grabbed headlines in recent months, with our top companies seeing intrusions and loss of data, and our constituents are beginning to realize that the internet is a highly contested space where personal information is never truly secure. What is not receiving much attention, however, is the fact that these incidents come from highly diverse actors, go after very different targets, and result in a broad range of consequences. The incidents range from what appears to be a new form of protest, referred to as "hacktivism," against soft targets such as the public websites of companies or government agencies, all the way to highly advanced nation-state actors involved in persistent and stealthy espionage of state secrets. The common thread is that the threats all exploit our strong reliance on the internet for social communication, business, and national defense, and will only increase as that reliance grows.

Let me first address an issue I believe Congress can easily support, once it receives the attention it deserves, and that is the crisis we are facing in highly skilled cybersecurity professionals. Our nation is a leader in internet security technology both in the private and federal sector, but we do not have enough highly trained individuals to match our growing needs. Nor do we have a strong pipeline for bringing talented individuals with an interest in computer security into the workforce. In 2008, Jim Gosler, the founder of the CIA's Clandestine Technology Office, estimated the U.S. only had 1000 security specialists with the advanced skills necessary to operate at a high level in cyberspace, while the number needed is closer to 20,000 or 30,000. However, since we have learned of this deficit, our workforce has stagnated, while the threat continues to multiply.

In Rhode Island, we are working to educate our future workforce for 21st century cybersecurity jobs. Earlier this year, we launched a pilot program with the Center for Internet Security to engage high school students in cybersecurity skills through competition. We had nearly 100 participants and local businesses offered internships to several of our winners. The University of Rhode Island also recently hosted a major symposium where federal, business, and academic leaders joined together to identify new areas for cyber research and development. As a result of this conference, we are building a statewide Cyber Center of Excellence that will work to grow the cyber workforce in Rhode Island, while meeting an increasing need for a strong public-private relationship in cyberspace.

As we prepare our workforce to meet these challenges, we must bring our laws and policies in line with the realities of today's internet, and I appreciate the Administration's proposals to move our nation in this direction. Since the first malware appeared in the early days of the internet, software has been created to offer a technical solution to make our systems and data more secure. Year after year this software has grown more complex, powerful, and expensive, while malicious code remains cheap and often easily procured. An analysis by the Department of Defense shows that since the late 1980's, the lines of code in security software have grown exponentially, while the lines of code in an average piece of malware have remained nearly constant. Unfortunately, this pattern shows that our security measures are divergent from the threat and that technical solutions alone are not enough to secure our valuable systems.

There are three policy areas under this Subcommittee's jurisdiction that I would particularly like to address: the White House's recommended penalties for cyber crime against critical infrastructure and racketeering; national data breach standards; and voluntary information sharing. While I understand that the Administration's proposal was intended to be taken as a whole product, I believe these three elements are especially important. As I discussed earlier, the foundations of trust and known identity on which the internet was built have enabled criminals to take advantage of those using the internet for commerce. Organized crime is fully operational online, stealing billions of real dollars every year to support worldwide networks of crime, yet the Racketeer Influenced and Corrupt Organizations (RICO), laws do not apply to cyberspace. The Administration has proposed allowing RICO to cover crimes committed in cyberspace, as well as setting mandatory minimum sentences for intrusions into critical infrastructure.

Similarly, recent incidents such as the Sony and Citibank intrusions have highlighted the large discrepancies in our data breach laws. Currently, each state is permitted to regulate when and how a company must disclose a breach of customer data to those affected. This regime makes little sense in cyberspace, where crimes and transactions take place at a national or international level. The Administration's proposals, as well as those introduced in the House and Senate, seek to set a federal standard for data breach notification. As we move to this model, however, we must also take care to implement the most effective -- not the lowest -- standard for reporting.

Finally, we must reexamine new opportunities for voluntary information sharing to ensure that we stop new threats before they reach their target. Today, our system of cyber-defense could be considered a digital Maginot Line. The government, businesses, and citizens all build their own digital fortifications and intruders maneuver to go around them. While the problem of attribution in cyberspace is always an issue, the government has a sophisticated understanding of the dangers we face. It also lacks the visibility of those in the private sector – telecommunications in particular - which can better pinpoint the source of the threat, or even stop it before it reaches our digital doorstep. This system is in place to today to help separate and protect our citizens' private data from being accessed unnecessarily by the government. But as the recent intrusions into Sony and other social networking sites have shown, the bad guys care little about privacy or security. Instead, we are losing the ability to stop attacks before they take place and provide better data security for everyone.

To address this issue without comprising privacy, the Administration proposes allowing cyber threat information to be shared voluntarily with the Department of Homeland Security, so that businesses, private citizens, and the government can all benefit from and be better protected by the increased capabilities and insight of an enhanced public-private partnership. In order for this arrangement to work, we must institute strict oversight to ensure that no personal communications or sensitive data are inappropriately shared with the government by businesses. This effort, if handled carefully and appropriately, could greatly enhance privacy by stopping malicious intrusions or large data theft efforts, and it is already under consideration by other partner countries as a way to provide a clearer picture of the health and security of the internet.

We are reaching critical mass, where our citizens are finally becoming aware of the threats that exist online, but a major catastrophe has not yet fallen on our digital shores. Inevitably, once such an event does occur, there will be strong and irresistible calls for broader measures that could overreact to a new threat. We must act now to implement sensible policies that enhance both security and privacy, before we are faced with a set of decisions that could fundamentally alter one of the most incredible tools of our time. I commend Senator Whitehouse for being a true leader on this issue as both a former member of the Senate Intelligence Committee and now Chairman of this Subcommittee. Thank you Mr. Chairman and Ranking Member Kyl for allowing me to testify today, and I look forward to working with you to help make the internet a stronger and more secure domain for all.