

**Statement of James R. Langevin (RI-02)**  
**Before the House Committee on Energy and Commerce,**  
**Subcommittee on Energy and Power**

**Legislative Hearing on “Protecting the Electric Grid: H.R. \_\_\_\_\_,**  
**the Grid Reliability and Infrastructure Defense Act”**

**May 31, 2011**

I would like to thank Chairman Whitfield and Ranking Member Rush for allowing me to testify on what I believe to be one of the most critical national security issues facing our country: securing our electric grid from cyber vulnerabilities. The Committee has given much attention to this topic over the past several years, and I commend you and your staff for your work. I previously testified on this issue in 2009 after a bill I had drafted with then-Homeland Security Chairman Bennie Thompson was adapted into then-Chairman Markey’s GRID Act, and I thank the committee for including me in this discussion again today.

Thirteen years ago, the President’s Commission on Critical Infrastructure Protection released a report on the risks associated with interconnected computer systems on the bulk power system. The Commission stated that “the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means.”

In the years since, we have seen this prediction validated as cyber threats across the power sector persist, along with an inability of industry to fully address these vulnerabilities on their own. One of the more public unclassified examples was seen in August 2003, when a software malfunction known as a “race condition” was set up in the control systems of a major East Coast energy supplier. This bug stalled their alarm systems after three power lines went down simultaneously, ultimately leading to a cascade failure of the entire Northeast power grid. The outage affected 55 million US and Canadian citizens and caused interruptions to water supplies, transportation systems, and cellular communications.

Unfortunately, cyber incidents on control systems aren’t limited to accidents. Press reports have detailed the shocking threats that our increasingly networked critical infrastructure could pose to our electrical grid.

The Wall Street Journal in 2009 reported that foreign adversaries had penetrated and mapped our electrical grid, potentially leaving behind software that could disrupt our systems. Another major cyber incident, the STUXNET worm, has more recently demonstrated that online actors are aware of the cyber vulnerabilities of critical infrastructure, and are able to design weapons to exploit them. Noting the fear that such a weapon could one day be leveled against American critical infrastructure, the acting director of DHS’s Cybersecurity Center noted that STUXNET “significantly changed the landscape of targeted cyberattacks.”

We know that there are a number of actors who seek to do harm to our networks -- from foreign nation states, to domestic criminals and hackers, to disgruntled employees. And as threats and capability grow, so does the risk of a cyber attack on our critical infrastructure.

This threat is not new. In 2009, I testified before this Subcommittee about the threats to our bulk power system from cyber attack, and I want to reiterate what I made clear in my previous testimony: I believe we remain vulnerable to a cyber attack against the electric grid that could cause severe damage to our critical infrastructure, our economy, our security and even American lives.

Federal agencies have taken steps to reduce these vulnerabilities, but I am afraid that many in industry -- and some in government -- still fail to appreciate the urgency of this threat. Since I began working on this issue, I have been disappointed by the overall lack of a serious response and commitment from the private sector. I held a hearing in 2007 examining the threats from an "Aurora"-like attack on our national power grid. At that time industry representatives lied to my Committee about having the situation fully under control. We caught them and they retracted their statements, but this attitude shows how difficult it can be to require and ensure security when it comes to critical infrastructure.

The vast majority of our critical assets are in private hands. In many sectors, private entities are largely self-regulated and are responsible for developing and implementing their own standards according to their own priorities. Because fixing vulnerabilities can be costly, security can find itself in conflict with other priorities like profit, competition, and accountability to shareholders. Sadly, the American people are the ones placed at risk when the owners of our critical infrastructure fail to prepare for worst-case scenarios.

I was pleased by the early attention paid to the issue of cybersecurity by the Obama Administration. In 2008, I worked with the transition team to highlight some cyber priorities from a congressional perspective, and it was clear even then that the incoming Administration understood the significance of the threat and planned to focus on the issue. Very soon after taking office, President Obama moved forward with the 60-day cyber review, becoming the first major world leader to take such action.

While progress has been slow at times, I would like to commend the Administration for taking some very serious steps in the right direction. Under the leadership of Cyber Coordinator Howard Schmidt and his staff, the White House has now released legislative guidance in response to much of the work already being done in Congress on this issue. Their recommendations envision more government involvement in setting standards and best practices for cyber protection across all sectors of our critical infrastructure, and mirror the philosophical framework of legislation I introduced earlier this year.

DHS has also taken important steps to become more involved in securing our critical infrastructure. The establishment of the Industrial Control Systems Computer Emergency Response Team, or ICS-CERT, under Sean McGurk, formalized a group of experts and fly-away teams that could respond to cyber incidents across all sectors of our utilities. However, a utility must first request help from the government before these resources can be brought to bear.

Unfortunately, the simple act of having to ask often forces decision makers in industry to steer clear of any government involvement for fear of embarrassment or competitive disadvantage. This leaves many owners and operators left to build piecemeal responses to what are often larger and highly sophisticated cyber problems.

I am pleased to see industry players increasingly stepping up to the plate to combat these threats, but I fear they cannot move fast or far enough under the current system. In discussing industry's current readiness to meet these new threats, Michael Assante, the president of the National Board of Information Security Examiners and former Chief Security Officer at the North American Electric Reliability Corporation (NERC) said, "We're not only susceptible, but we're not very well prepared." Threats like STUXNET have been a wake-up call, and the time is right for government to work with industry partners to address the shortfalls in our current regulatory regime.

I supported the GRID Act as it moved through the House last year, because it seeks to address some of the unique regulatory challenges in our power industry today. Currently we live under a system that does not prioritize security, but actively penalizes open reporting and cooperation. The legislation aims to correct this by allowing Federal regulators greater authority to protect Americans during times of imminent crisis. It also provides for the issuance of orders to identify and mitigate vulnerabilities to protect the bulk power system and defense critical electric infrastructure (DCEI) from cyber attacks, direct physical attacks, manmade EMP, and geomagnetic storms.

While this measure is a significant step forward, I would also strongly encourage the Committee to consider provisions in my legislation, and in Senate and Administration proposals, that expand this model to other sectors of critical infrastructure and enhance the ongoing efforts of DHS to quickly respond to a major crisis. I would also note my concern that by specifying only the "bulk power system," this legislation excludes critical distribution systems that would leave major cities, like New York and Washington, D.C., unprotected by the broader provisions in the bill.

I'll conclude by cautioning again that inaction on this issue will make our nation increasingly vulnerable to cyber attacks, from both outside and within. We know the threat exists and we have an opportunity to address it before any further damage is caused. It is the responsibility of Congress and the Administration to take the appropriate steps that will protect this nation.

I want to once again thank Chairman Whitfield and Ranking Member Rush for their attention to this important issue and for the opportunity to testify. I look forward to working with the Energy and Commerce Committee and to supporting your efforts to raise awareness about securing our critical infrastructure and protecting our citizens from cyber attack. Thank you.