

Subcommittee on Energy and Air Quality hearing, "Protecting the Grid From Cybersecurity Threats."

Today's hearing focuses on how to help ensure the reliability of our Nation's electricity grid in the face of its vulnerabilities to cybersecurity attacks.

Subcommittee on Energy and Air Quality hearing, "Protecting the Grid From Cybersecurity Threats," September 11, 2008

Today's hearing focuses on how to help ensure the reliability of our Nation's electricity grid in the face of its vulnerabilities to cybersecurity attacks.

A successful remote cyber attack on a power plant's utility control systems could do more than cause a brief black out or brown out. The Idaho National Laboratories has shown how a hacker can remotely turn a large generator into a smoldering piece of scrap metal in minutes. Known as the "Aurora" Vulnerability, this type of attack could destroy generating equipment and impair the generation and delivery of electricity across North America for weeks or months, its consequences cascading on consumers, our economy, our health care system, and our national defense assets.

These concerns are more than theoretical. A 2005 Federal Energy Regulatory Commission staff report identified 20 separate domestic and foreign instances of cyber attacks on electricity systems including hydroelectric dams and nuclear power plants. The Defense Science Board reports that U.S. grid control systems are continuously probed electronically, and "there have been numerous attempted attacks on the Supervisory Control and Data Acquisition (SCADA) systems that operate the grid."

We have been fortunate that the United States has not experienced a major power outage from a cyber attack. However, the CIA has identified cyber attacks on the electrical systems in major cities overseas which caused significant blackouts. CIA has reported that criminal enterprises have broken into utility control systems overseas as part of extortion schemes.

Since many of these same control systems used in the United States are also used in plants around the world, the knowledge about how these systems work is globalized.

In response to Department of Homeland Security's warnings about the Aurora vulnerability, the North American Electric Reliability Corporation (NERC) issued an advisory in June 2007 which outlined immediate and longer term mitigation measures for utilities. Compliance, however, was voluntary.

A FERC audit of 30 utilities found that only two or three had adequately mitigated the Aurora vulnerability and the vast majority had not complied with NERC's advisory. For some of the Nation's largest utilities, there has been woeful inaction some 15 months later.

As the Electricity Reliability Organization designated under Section 215 of the Energy Policy Act of 2005, NERC is developing consensus cyber protection standards. However, this process is not responsive to the immediacy of the vulnerability or the threat. Both the Department of Energy and FERC have urged that Congress extend Federal authority to take emergency actions to protect the grid.

I commend Chairman Boucher for holding this hearing, and tackling the job of building a bipartisan consensus on legislation which will ensure that the Federal Government has the necessary powers to intervene when there are emergencies that threaten our Nation's electricity supply.

I welcome Representative Jim Langevin, Chairman of the Homeland Security Committee's Subcommittee on Emerging Threats, Cybersecurity and Science and Technology, and commend him for his leadership and cooperation in working with this Committee on cyber vulnerabilities in the utility grid.

I also welcome our panel of witnesses. I hope they can inform us on whether emergency powers should extend beyond the Bulk Power System to utility systems in Alaska, Hawaii, or Guam, and to what extent these powers should also be able to reach critical distribution systems in places like the District of Columbia or New York City. We want to be sure that legislation addresses threats to the electrical system, and that the Federal Government is not improperly hobbled by legal and jurisdictional boundaries in the case of an

emergency.

Prepared by the Committee on Energy and Commerce

2125 Rayburn House Office Building, Washington, DC 20515