



The Committee on Energy and Commerce

Internal Memorandum

May 26, 2011

TO: Members, Subcommittee on Energy and Power

FROM: Committee Staff

RE: Hearing on “Protecting the Electric Grid: H.R.____, the Grid Reliability and Infrastructure Defense Act”

On Tuesday, May 31, 2011, at 2:00 p.m. in Room 2123 of the Rayburn House Office Building, the Subcommittee on Energy and Power will hold a legislative hearing entitled: “Protecting the Electric Grid: H.R.____, the Grid Reliability and Infrastructure Defense Act.” A discussion draft of this legislation was released on May 23. Witnesses are expected to testify on the proposed legislation and provide testimony pertaining to protecting the bulk power system from physical and cyber threats and vulnerabilities.

I. WITNESSES

The invited witnesses are:

Panel I

The Honorable Trent Franks
Arizona 2nd District
U.S. House of Representatives

Panel II

The Honorable Patricia A. Hoffman
Assistant Secretary, Office of Electricity
Delivery and Energy Reliability
U.S. Department of Energy

The Honorable Paul N. Stockton
Assistant Secretary of Defense for Homeland
Defense and America’s Security Affairs
U.S. Department of Defense

Mr. Joseph H. McClelland
Director, Office of Electric Reliability
Federal Energy Regulatory Commission

Panel III

Mr. Gerry Cauley
President and CEO
North American Electric Reliability Corp.

Mr. Barry Lawson
Associate Director, Power Delivery &
Reliability
National Rural Electric Cooperative Assoc.

Mr. Franklin D. Kramer
Fmr. Assistant Secretary of Defense for
International Security Affairs
U.S. Department of Defense

II. BACKGROUND

The U.S. electric grid is a vast network of interconnected transmission lines, local distribution systems, generation facilities, and related communications systems. The bulk-power system in the United States and Canada has more than 200,000 miles of transmission lines, has more than 800,000 megawatts of generating capacity, is valued at over \$1 trillion, and serves more than 300 million people.

Public reports relating to cyber vulnerabilities and threats to the electric grid have increased in recent years and were the subject of several hearings in the 110th and 111th Congresses. In addition, it has been reported that actors based in China, Russia, and other nations have conducted cyber ‘probes’ of U.S. grid systems, and that cyber attacks have been conducted against critical infrastructure in other countries.

In addition to potential cyber attacks, there is a growing concern of physical vulnerabilities and threats to the grid, including:

- Physical Attacks to Critical Energy Infrastructure: A direct physical attack on critical grid infrastructure would disrupt the nation’s electricity supply, thus exposing the nation to significant physical and economic harm.
- Electromagnetic Pulse (EMP): There are three general categories of EMP: (1) geomagnetic storms resulting from solar activity; (2) intentional electromagnetic interference that could destroy or temporarily disable electronic equipment; and (3) high-altitude detonation of a nuclear weapon.
- Unavailability of Large Transformers: Large transformers are essential to the reliable operation of the grid but are manufactured outside of the U.S. and replacement may require two years or longer. Should an attack or event occur, it is imperative that the U.S. have a reliable supply of large transformers to replace damaged or destroyed equipment.

III. THE GRID ACT

Last Congress, Mr. Upton and Mr. Markey co-sponsored the Grid Reliability and Infrastructure Defense Act (H.R. 5026) (the “GRID Act”) to protect critical electric infrastructure from various threats and vulnerabilities. After being reported favorably by the Energy and Commerce Committee (47-0), the House passed the GRID Act by voice vote on June 9, 2010.

The discussion draft of the GRID Act is identical to last year’s bill. The legislation aims to protect the bulk power system and defense critical electric infrastructure (DCEI) from cyber attacks, direct physical attacks, manmade EMP, and geomagnetic storms. Upon notice from the President of an imminent grid security threat, the Federal Energy Regulatory Commission (FERC) may issue orders for emergency measures as it determines necessary to protect the reliability of the bulk power system or DCEI. In addition, the bill provides FERC greater authority to issue orders to identify and mitigate reliability vulnerabilities. The GRID Act also requires FERC to direct the North American Electric Reliability Corporation (NERC) to develop reliability standards addressing the availability of large transformers.

Section 1: Short Title

Section 1 provides the short title for the legislation, the “Grid Reliability and Infrastructure Defense Act” or the “GRID Act.”

Section 2: Amendment to the Federal Power Act

Section 2 provides FERC with emergency cyber and physical authority over the bulk power system, pursuant to a Presidential declaration of an imminent threat to grid security. FERC also is authorized to conduct its own rulemaking for the bulk power system to address cyber and EMP vulnerabilities. It provides FERC emergency and cyber vulnerability rulemaking authority over distribution-level facilities that serve DCEI. It establishes NERC rulemakings, at the direction of FERC, to address large transformer supply and geomagnetic storms. It directs the President to designate not more than 100 facilities that are critical to U.S. national security and that are served by DCEI. It addresses the treatment of “protected information” and establishes a program at the Department of Energy to develop technical expertise in the protection of the grid against various threats.

Section 3: Budgetary Compliance

To the extent applicable, Section 3 ensures compliance with the Statutory Pay-As-You-Go Act of 2010.

IV. ISSUES

The following issues will be examined at the hearing:

- The type of threats facing the bulk power system and DCEI;
- Current weaknesses that leave the bulk power system and DCEI vulnerable to physical or cyber attacks or events;
- The national security and economic implications potentially resulting from an attack or event affecting the bulk power system or DCEI;
- The activities presently being undertaken to address grid vulnerabilities;
- Ways to improve cooperation and communication between government agencies, owners and operators of the bulk power system, and other stakeholders;
- The discussion draft's goal of addressing grid security threats and vulnerabilities; and
- Whether the GRID Act requires revision to reflect current conditions or changed circumstances.

V. STAFF CONTACTS

If you have any questions regarding this hearing, please contact Patrick Currier at 5-2927.