The Committee on Energy and Commerce

Internal Memorandum

February 23, 2012

TO: Members, Subcommittee on Oversight and Investigation

FROM: Subcommittee on Oversight and Investigations Staff

RE: Hearing on "Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security"

On Tuesday, February 28, 2012, at 10:15 a.m. in room 2322 of the Rayburn House Office Building, the Subcommittee on Oversight and Investigations will hold a hearing entitled "Critical Infrastructure Cybersecurity: Assessments of Smart Grid Security." The hearing will provide an overview of the federal government's efforts to protect critical infrastructure, such as the electric grid, against cyber threats and a discussion of current cyber threats and risks. The hearing will examine cybersecurity threats to the Smart Grid and examine weaknesses that make the Smart Grid vulnerable to attacks. In particular, the Subcommittee will examine the challenges the Department of Energy (DOE) faces as it works to invest in and protect these infrastructures. This hearing will be the second in a series of hearings that focuses on the cybersecurity threats related to infrastructure and industries within the jurisdiction of the Energy and Commerce Committee.

I. WITNESSES

Three witnesses will testify at the hearing:

Gregory C. Wilshusen
Director of Information Security Issues
Government Accountability Office (GAO)

David Trimble
Director, Natural Resources and Environment
Government Accountability Office (GAO)

Richard J. Campbell
Specialist in Energy Policy
Congressional Research Service (CRS)

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. The Smart Grid refers to the evolving electric power network that incorporates information technology systems and capabilities through modernization. These technologies and capabilities help collect, analyze and distribute behavioral information to influence the control of power flow and enhance efficiencies and reliability of the existing grid. The interoperability of these systems makes them more susceptible to cybersecurity issues.

Smart Grid technologies are designed to lower operation costs, reduce maintenance costs, and expand the flexibility of operational control relative to the current grid system. While increased energy efficiency is achieved by operational efficiency and improved asset utilization, cybersecurity impacts the advanced communications and information technologies deployed within these systems. To achieve these goals, a clear direction is necessary.

Cybersecurity is a critical issue for electrical utilities to identify and implement along with other priorities as they begin to modernize the electric grid. Cybersecurity threats represent a constant moving target and mitigation of those threats creates an ever-moving challenge for electrical utilities to address. While cyber-intrusions into the electrical grid have been reported in recent years and are likely to increase, the government has taken steps to ensure critical infrastructure is protected.

III. ISSUES

The following issues will be examined at the hearing:

- The current risks and threats to cybersecurity, particularly infrastructures within this Committee's jurisdiction including the electric utility grid, and how this impacts efforts to protect critical infrastructure.

- Are there clear goals for the use of Smart Grid funds and do those goals include cybersecurity priorities? Have these efforts resulted in improved cybersecurity?

- Can the Smart Grid strengthen cybersecurity and achieve the level of interoperability necessary to make an efficient and reliable electric system?

IV. CONTACTS

If you have any questions about this hearing, please contact Carl Anderson at (202) 225-2927.