



FOR IMMEDIATE RELEASE

Statement of Chairman Bennie G. Thompson

Securing the Modern Electric Grid from Physical and Cyber Attacks

July 21, 2009 (Washington) – Today, Committee on Homeland Security Chairman Bennie G. Thompson (D-MS) delivered the following prepared remarks for the full Committee hearing entitled “Securing the Modern Electric Grid from Physical and Cyber Attacks”:

“A multitude of failures contributed to our inability to prevent the attacks on New York City and Washington, D.C. on September 11th. Mindful of our previous mistakes, let’s review the set of facts before us in today’s testimony:

- We have significant vulnerabilities in the grid’s electronic infrastructure;
- The infrastructure is only getting more vulnerable with Smart Grid technology;
- There is a massive computer espionage campaign being launched against the United States by our adversaries;
- Intelligence suggests that countries seek or have developed weapons capable of destroying our grid;
- A Congressional Commission says that our grid and the critical infrastructure that relies on the grid is not adequately protected;
- Our military installations are vulnerable because they rely on an insecure electric grid;
- The private sector is in charge of writing its own security standards, but experts have judged the standards to be ineffective in securing the infrastructure; and
- Many utilities are avoiding compliance with the standards.

I ask my colleagues here today, and those who could not join us: what more do we need to hear before we act? What more motivation do we need? The warning signs are flashing red. Now is the time to act to secure the electric grid, not after a major incident has occurred.

This Committee has a bipartisan, bicameral legislative solution to secure the electric grid. Our bill is comprehensive in its scope. Because the grid is only as strong as its weakest link, we believe that all elements of the grid – from generation to transmission to distribution to metering infrastructure – should be included. Our bill covers physical attacks – like electromagnetic pulse – as well as cyber attacks.

The Critical Electric Infrastructure Protection Act will do four things to improve our defensive posture. It requires FERC to establish interim measures deemed necessary to protect against physical and cyber threats to critical electric infrastructure. This will improve existing mandatory standards. It provides FERC with the authorities necessary to issue emergency orders to owners and operators of the electric grid after receiving a finding from DHS about a credible and imminent cyber attack.

It requires DHS to perform ongoing cybersecurity vulnerability and threat assessments to the critical electric infrastructure, and provide mitigation recommendations to eliminate those vulnerabilities and threats. And it requires DHS to conduct an investigation to determine if the security of Federally-owned critical electric infrastructure has been compromised by outsiders.

I’m proud of this bill. I know my colleagues are proud of this bill. We have the support of nearly 30 Republican and Democratic co-sponsors, and we’re looking for more.

For years, experts have been warning us about the grid. The time for action is long overdue. I thank the Chair for her concern and leadership, and look forward to working with her, the Committee, and the Energy and Commerce Committee in moving this legislation forward.”

#

FOR MORE INFORMATION: Please contact Dena Graziano or Adam Comis at (202) 225-9978

United States House of Representatives
Committee on Homeland Security
H2-176, Ford House Office Building, Washington, D.C. 20515
Phone: (202) 226-2616 | Fax: (202) 226-4499
<http://homeland.house.gov>