



**One Hundred Eleventh Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515**

**Protect the Grid from Cyber Attack:
Co-sponsor HR 2195, the Critical Electric Infrastructure Protection Act**

May 6, 2009

Dear Colleague:

As sponsors of H.R. 2195, the "Critical Electric Infrastructure Protection Act," we invite you to cosponsor this bill which will secure the U.S. electric grid from cyber attack.

The effective functioning of our electric grid is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet.

Intentional and unintentional control system failures on the electric grid can have a significant and potentially devastating impact on the economy, public health, and national security of the United States. For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, and water systems presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over \$700 billion.¹ Failures on the grid could also severely impact the ability of our war fighting capability. In a report titled, "More Fight – Less Fuel" issued in February 2008, the Defense Science Board concluded that "critical national security and homeland defense missions are at an unacceptably high risk of extended outage from failure of the grid and other critical national infrastructure."²

An article in the April 8, 2009 edition of the *Wall Street Journal* reported that "cyberspies have penetrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system, according to current and former national security officials."³ According to the article, spies from China, Russia, and other countries were believed to be on a mission to navigate the U.S. electrical system and its controls. "The

¹ (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from <http://www.cnn.com/2007/US/09/27/power.at.risk/index.html>.

² Report of the Defense Science Board Task Force on DOD Energy Strategy, *More Fight – Less Fuel*, February 2008, available at <http://www.acq.osd.mil/dsb/reports/2008-02-ESTF.pdf>.

³ "Electricity Grid in U.S. Penetrated by Spies," *Wall Street Journal*, Apr. 8, 2009.

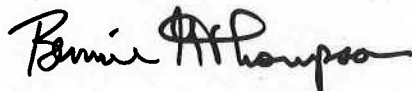
intruders haven't sought to damage the power grid or other key infrastructure, but officials warned they could try during a crisis or war."⁴

We are proposing a common-sense legislative approach to ensure that our electric infrastructure is secure. The Critical Electric Infrastructure Protection Act:

- Requires the Secretary of Homeland Security to perform ongoing cyber threat and vulnerability assessments of the critical electric infrastructure.
- Provides authority to the Federal Energy Regulatory Commission (FERC) to issue emergency rules or orders to address imminent cyber threats or cyber vulnerabilities.
- Requires FERC to assess and establish interim standards deemed necessary to protect against known cyber threats to critical electric infrastructure that are otherwise not covered by existing mandatory standards.
- Requires DHS to conduct an investigation to determine if the security of Federally-owned critical electric infrastructure has been compromised by outsiders.

Please contact Jacob Olcott, majority staff of the Homeland Security Committee at 226-2616 or Coley O'Brien, Republican staff, at 226-8417 if you have any questions or would like to be a cosponsor.

Sincerely,



BENNIE G. THOMPSON
Chairman



PETER T. KING
Ranking Member

⁴ *Id.*