COMMITTEES

ENERGY AND COMMERCE
SUBCOMMITTEE ON
ENERGY AND ENVIRONMENT
CHAIRMAN

SELECT COMMITTEE ON
ENERGY INDEPENDENCE AND
GLOBAL WARMING
CHAIRMAN

NATURAL RESOURCES

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900

http://markey.house.gov

April 9, 2009

The Honorable Jon Wellinghoff
Chairman
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Dear Chairman Wellinghoff:

I have long been concerned about threats to our energy infrastructure, from terrorist attacks on LNG facilities to assaults on nuclear power plants from the air or the ground. Recent reports raise concerns about a more modern threat: cyber attack to our nation's electricity generation and transmission infrastructure. This matter warrants serious attention and I ask your assistance as we investigate the nature of the threat and what can be done to repel it.

As you know, the North American Electric Reliability Corporation, which is mandated to ensure the reliability of the nation's electricity supply, recently completed a survey of industry stakeholders to determine compliance with the Critical Cyber Asset Identification Standard. The results of this survey raise two issues of serious concern. First, the survey makes clear that industry has not fully adhered to this Standard, which is only concerned with identifying – not defending – facilities and equipment critical to the reliability of the electrical supply. This lack of adherence by industry to the Standard is disturbing because it indicates the vulnerability of the nation's electrical grid to cyber attack. If we have not yet even identified which assets need to be defended from cyber attack, how can we possibly defend them?

The second, and more disturbing, concern arises from recent news reports that the computer-based infrastructures of the grid have been repeatedly and systematically compromised through the Internet by foreign nations and groups. All Americans are troubled to learn that foreign nations and potentially hostile groups are apparently preparing a detailed "map" of the grid and its vulnerabilities, possibly to be used to facilitate some sort of attack in the future.

In light of these reports on growing threats to our electrical grid, I request additional information on what steps the Federal Energy Regulatory Commission (FERC) is taking to respond to these threats in the near term and prevent such breaches in the future.

In January of 2008, FERC approved eight mandatory critical infrastructure protection (CIP) standards, as developed by the North American Electric Reliability Corporation, to protect the nation's grid from cyber security attacks and other reliability breaches. The mandatory reliability standards required certain users, owners and operators of the bulk power system to

establish policies, plans and procedures to safeguard physical and electronic access to control systems, to train personnel on security matters, to report security incidents, and to be prepared to recover from a cyber incident. These standards were to provide a "comprehensive set of requirements to protect the Bulk-Power System from malicious cyber attacks."

Please answer the following questions regarding FERC's actions in response to these threats and what additional measures may need to be taken by the industry, the Commission, and by Congress.

- What is the Commission's view of the results of the North American Electric Reliability Corporation survey? What percentage of Critical Cyber Assets have been identified? What is the significance of the information backbone of the electric grid being compromised? What immediate steps is the industry taking to stop these breaches?
- If foreign nations or hostile groups already have gathered detailed information to develop a "map" of the electricity grid, what actions can be taken now to prevent this information from being used to attack the grid?
- Have the CIP standards been fully implemented by industry? If not, why not?
- Are the current CIP standards sufficient to prevent cyber-security attacks and to respond to breaches? If not, what additional standards are needed?
- Has FERC developed metrics to measure the efficacy of the CIP standards? If so, what are these metrics? If not, why not?
- What processes are on-going at NERC to identify the need for new cyber-security standards?
- Is too much discretion given to industry participants in creating the cyber-security standards, since two-thirds of the group's members must support a standard before it is adopted or modified?
- What authorities does FERC possess to prevent and respond to cyber-security threats and breaches? Does FERC need additional authorities to protect the electricity grid from these threats?

Thank you for the attention to these matters. If you have any questions regarding this request, please contact Will Huntington of my staff at 202-225-2836.

Sincerely,

Edward J. Markey

Edward J. Markey
Chairman
Subcommittee on Energy and
The Environment