INSTITUTE FOR 21ST CENTURY ENERGY
U.S. CHAMBER OF COMMERCE

Karen Alderman Harbert
President and CEO

1615 H Street, NW | Washington, DC 20062
(202) 463-5558 | (202) 887-3457 Fax
www.energyxxi.org

March 24, 2014

Ms. Kimberly D. Bose
Federal Energy Regulatory Commission
888 First Street NE, Room 1A
Washington, DC 20426

Re: FERC Notice of Proposed Rulemaking, *Reliability Standard for Geomagnetic Disturbance Operations, Docket No. RM14-1-000*

Dear Ms. Bose:

The Institute for 21st Century Energy (the "Energy Institute"), an affiliate of the U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses and organizations of every size, sector and region, submits these comments in response to the January 16, 2014, issuance by the Federal Energy Regulatory Commission ("Commission") of a Notice of Proposed Rulemaking issued in Docket No. RM14-1-000 that proposes to approve a reliability standard aimed at mitigating the effects of a geomagnetic disturbance on the Bulk-Power System (the "GMD NOPR"). The Energy Institute supports both the process and the product related to Reliability Standard EOP-010-1 (Geomagnetic Disturbance Operations), and thus supports the standard's proposed adoption.

The actual impact that a significant geomagnetic disturbance – or GMD event – could have on the electric grid and the components thereof, either from a solar flare or alternate triggering device, remains largely conceptual. While some equipment suppliers claim to have the silver bullet necessary to protect against these types of events, it is unclear whether these proposed "solutions" would serve to insulate the grid or instead make aspects of the grid more vulnerable to the forces resulting from a GMD event. Nevertheless, consistent with the Energy Institute's recommendation within its recently-released "Energy Works for US" policy platform, it is essential that the industry, in cooperation with relevant governmental entities, develop a greater understanding and associated expertise regarding the potential vulnerabilities that may exist within the Bulk-Power System to a significant GMD event. Attached to these comments please find our "two pager" document that summarizes the Energy Works for US chapter, and associated recommendations, on physical and cyber risks to energy infrastructure.

The Energy Institute believes that the GMD NOPR moves the needle in the correct direction by proposing to adopt a standard that was developed through the stakeholder standards development process administered by the North American Electric Reliability Corporation

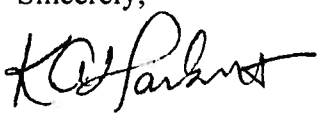
(NERC). As a result, the standards reflect informative outreach to industry and the technical expertise residing therein, and result in a standard that is purposely not prescriptive in nature. Rather, the standard appropriately provides individual owners and operators of covered infrastructure the latitude to determine the operating processes and procedures that work best for their specific situation and system in the face of a GMD event.

The GMD NOPR is also commendable because it supports information sharing with respect to the requirement that reliability coordinators disseminate space weather information. This approach is consistent with the information sharing recommendations that the Energy Institute has also advocated with respect to the strategies that should be implemented to protect the electric grid from malicious cyber intrusions. While cyber security differs in certain aspects as compared to the threats posed by a GMD event, the benefits that can accrue from the sharing of actionable information, among the right people, in a timely manner, holds true in each domain. The GMD NOPR moves in this direction, even though it involves the dissemination of publicly available information to the system operators and reliability coordinators that would need to take protective action with Bulk Power System equipment during a GMD event.

The GMD NOPR appropriately proposes to approve a non-prescriptive standard that provides for the flexibility that is necessary to enable electric system owners and operators to best protect the unique equipment and system configurations that exist across the interconnected electric grid. The Commission should be commended for proposing to approve the adoption of Standard EOP-010-1, because it will enhance the reliability of the Bulk-Power System.

We appreciate your consideration of the Energy Institute's comments, herein, as part of the above-captioned rulemaking process.

Sincerely,



Karen A. Harbert

Enclosure

Protect Our Energy Infrastructure from Physical Disruptions and Cyber Attacks

ENERGY Works For US

A reliable grid is essential to U.S. energy security. New threats have emerged to our energy infrastructure in the form of cyber attacks and the potential for geomagnetic storms. Computer networks that control infrastructure are repeatedly attacked. To combat these challenges, information exchanges between government intelligence agencies and the private sector should be enhanced.

Cyber Incidents by Sector: Fiscal Year 2012

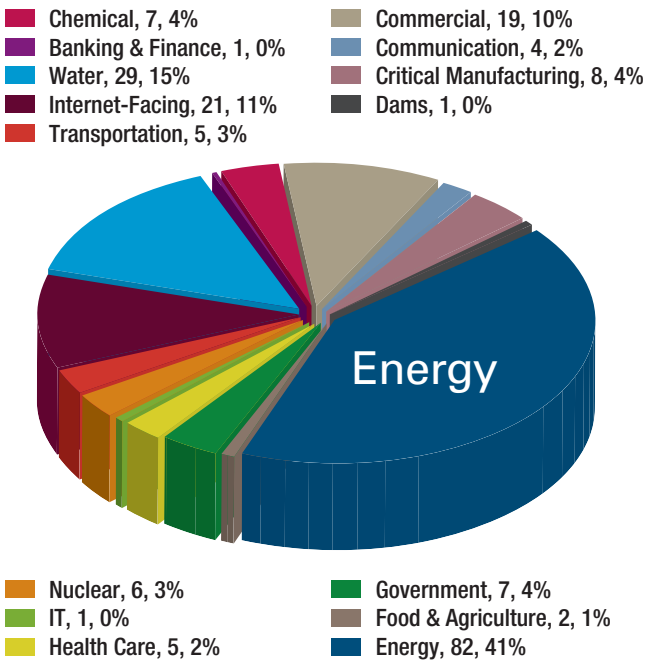


Image source: DHS Industrial Control Systems Cyber Emergency Response Team, ICS-CERT Monitor

Policy Recommendations

- Congress should enact legislation supporting the exchange of threat information between the government intelligence community and the private-sector owners and operators of critical energy infrastructure. Such legislation should include full liability protections and codify narrowly tailored measures to help business owners and operators harden critical infrastructure and adopt cutting-edge cybersecurity practices that serve to strengthen industry-specific efforts.
- Congress should direct DHS, in cooperation with DOE, to study the potential impacts of geomagnetic and electromagnetic disturbances on energy infrastructure and implement reasonable risk-based plans to insulate critical facilities from such threats in a cost-effective manner.

Securing the U.S. Energy Grid

DHS recently reported that in fiscal years 2011 and 2012, cyber attacks targeting energy and pipeline infrastructure were increasing around the world. According to the agency, cyber intrusions into pipeline and electric power infrastructure have been occurring at an "alarming rate," with attacks against energy-related systems comprising more than 40% of all reported incidents in fiscal year 2012.

The energy sector is one of the key infrastructure sectors identified in the National Infrastructure Protection Plan, now overseen by DHS. Through this framework, sector-specific plans are developed and implemented, providing cyber and physical infrastructure and supply-chain protections that are crafted to match sector-specific characteristics and conditions.

On February 12, 2013, the White House issued an executive order directed at improving critical infrastructure cybersecurity.

The executive order rightly elevates the importance of bidirectional information sharing, and it also calls on government officials to produce timely classified and unclassified reports on cyber threats for specific targets, such as U.S. critical infrastructure.

Legislation should codify and build upon these advances by providing legal certainty that businesses which voluntarily share threat information with the government will be provided safe harbor against the risk of frivolous lawsuits, will be exempt from public disclosure, and that cyber threat information will not be subject to use by government officials to regulate other activities.

With respect to the protection of critical energy infrastructure from threats such as geomagnetic and electromagnetic disturbances, an established public-private partnership with active and largely uninhibited information-sharing can also pay dividends. And in the case of an electromagnetic attack, the Department of Defense plays a primary role in prevention.

MORE THAN

80%

OF THE NATION'S ENERGY INFRASTRUCTURE IS OWNED AND OPERATED BY THE PRIVATE SECTOR.

ATTACKS AGAINST ENERGY-RELATED SYSTEMS COMPRISED MORE THAN

40%

OF REPORTED INCIDENTS IN FY 2012.

From October 2009 to March 2012, the Department of Energy recorded

2,300

INCIDENTS

OF "UNAUTHORIZED COMPUTER ACCESS, IMPROPER USE OF COMPUTING RESOURCES AND THE INSTALLATION OF MALICIOUS SOFTWARE."

Want to know more about cyber security? Read the full report, *Energy Works for US*.

ENERGY Works For US

www.energyxxi.org/energyworksforus

Data referenced from the following sources: Department of Homeland Security; Department of Energy