U.S. CHAMBER OF COMMERCE

Ann M. Beauchesne
Senior Vice President
National Security and Emergency Preparedness

1615 H Street, NW
Washington, DC 20062
202-463-3100

February 26, 2018

Kimberly Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426

Subject: *Cyber Security Incident Reporting Reliability Standards* (Docket No. RM18-2-000)

Dear Secretary Bose:

The U.S. Chamber of Commerce welcomes the opportunity to respond to the Federal Energy Regulatory Commission's (FERC's) request for comments on its notice of proposed rulemaking *Cyber Security Incident Reporting Reliability Standards*.[1]

The Chamber respects FERC's interest in obtaining an accurate picture of cyber risks that could impact the reliable operation of the bulk electric system (BES). North American Electric Reliability Corporation (NERC) entities also need quality, timely cyber threat data, some of which are only obtainable from governmental sources. Our organization strongly supports voluntary, protected cybersecurity information-sharing programs. It believes that FERC should resist calls to direct NERC to modify the Critical Infrastructure Protection (CIP) Reliability Standards to compel more reporting by industry.

Nevertheless, the Chamber believes that a positive outcome is achievable between FERC and NERC stakeholders. Instead of mandating additional reporting, FERC should explore opportunities with industry to support the existing voluntary cybersecurity information-sharing programs. An optimal and sustainable outcome would contain the following principles and objectives:

- **Mandatory cyber incident reporting does not strengthen cybersecurity.** More forced reporting is likely to create substantial noise in the system and lead to a diffusion of NERC members' limited resources toward compliance and away from risk management activities.[2]

- **Information sharing needs to be rooted in reciprocity.** NERC and industry parties should voluntarily exchange threat data concerning potential and actual cyberattacks. Information sharing should be a two-way street—one where threat data flow

to businesses from government and vice versa. The agency's rulemaking does not address how reported cyber information would tangibly benefit electric utilities and other industry actors.

- **NERC entities should have reasonable control over the handling of shared threat information.** Designations (e.g., the Traffic Light Protocol) identify unclassified information that may not be suitable for public release and could require special handling.[3]

- **Electric-sector parties need security clearances.** Despite a well-known backlog in the security clearance process, many electric-sector entities that are covered by the CIP standards need security clearances. FERC's proposed rulemaking does not account for how the agency's call for enhanced information is at odds with the incredibly slow background investigation process.[4]

- **NERC stakeholders need access to classified threat data and closer collaboration with federal agencies and industry peers.**[5] Private parties, put simply, need to become a customer of the intelligence community (IC) as part of an overall solution to boosting U.S. cybersecurity. Electric-sector entities must be able to receive classified threat information in real time and coordinate securely with government and other private companies on network defense.[6] Increasing productive interactions between self-selected industry actors and the IC regarding cybersecurity is a top Chamber objective.

- **FERC actions should foster, not impede, industry's use of leading cyber technologies.** The agency's suggested regulatory changes could slow innovative approaches to cybersecurity among electric utilities, which would be troubling to the Chamber. NERC entities may opt to leverage technology vendors (e.g., cloud computing providers) to improve service operations and reliability for functions that may not operate BES directly but integrate closely with such systems and could be considered an extension of electricity providers.[7]

- **Public-private response coordination needs tightening.** NERC entities need confidence that public and private stakeholders are clear about their roles and responsibilities. The Chamber recognizes that cyberattacks cannot be handled solely by government, but cyberspace is the only domain where the government asks private companies to defend themselves against foreign powers and other significant threats, which is unworkable in many instances.[8]

***

The Chamber appreciates the opportunity to offer its views to FERC on constructive ways to address cybersecurity incident reporting. If you have any questions or need more information, please do not hesitate to contact me (abeauchesne@uschamber.com, 202-463-3100) or my colleague Matthew J. Eggers (meggers@uschamber.com, 202-463-5619).

Sincerely,

Ann M. Beauchesne
Senior Vice President

Matthew J. Eggers
Executive Director, Cybersecurity Policy

Endnotes

[1] www.federalregister.gov/documents/2017/12/28/2017-28083/cyber-security-incident-reporting-reliability-standards

www.ferc.gov/media/news-releases/2017/2017-4/12-21-17-E-1.asp#.WoCvVUly6Uk

[2] www.gao.gov/products/GAO-08-904T

www.uschamber.com/sites/default/files/documents/files/oct_20_letter_to_wh_cyber_commission_re_sec_pritzker_address_final.pdf

[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf

[4] www.gao.gov/products/GAO-18-29?utm_medium=email&utm_source=govdelivery

[5] www.dhs.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf

[6] http://docs.house.gov/meetings/HM/HM08/20171115/106632/HHRG-115-HM08-Wstate-KnakeR-20171115.pdf

www.insaonline.org/wp-content/uploads/2017/06/INSA-FINnet-Proposal-June-2017.pdf

http://docs.house.gov/meetings/AS/AS00/20170301/105607/HHRG-115-AS00-Bio-HealeyJ-20170301-U1.pdf

www.congress.gov/bill/114th-congress/senate-bill/3017

www.congress.gov/bill/115th-congress/senate-bill/133

www.energy.gov/articles/secretary-energy-rick-perry-forms-new-office-cybersecurity-energy-security-and-emergency

[7] Prior to introducing modifications to the CIP standards, FERC should convene NERC stakeholders and the vendor community. This group could discuss the anticipated impacts of the rulemaking, the agency's desired outcomes, and the capabilities and investments of both regulated entities and third-party providers. Such a dialogue would provide an alternate way to achieve FERC's desired outcomes.

[8] www.uschamber.com/sites/default/files/documents/files/10-31-16_uscc_letter_re_draft_ncirp_final.pdf