



July 16, 2015

News Media Contact

Mary O'Driscoll | 202-502-8680

Docket No. RM15-14-000

Item No. E-1

FERC Eyes Development of Supply Chain Cyber Controls in New Reliability Standards

The Federal Energy Regulatory Commission (FERC) acted today to improve the cyber security of the bulk electric system by proposing revisions to critical infrastructure protection (CIP) Reliability Standards to address risks to communication networks and related bulk electric system assets and the development of standards for supply chain management security controls to protect the bulk electric system from security vulnerabilities and malware threats.

The revisions are included in a Notice of Proposed Rulemaking that seeks comment on seven updated CIP Reliability Standards proposed by the North American Electric Reliability Corporation (NERC). NERC is the Commission-certified electric reliability organization, and the new Reliability Standards would address issues ranging from personnel and training to physical security of the bulk electric system's cyber systems and information protection. The Commission's proposal would modify the scope and applicability of certain CIP Standards to protect communication links and sensitive data among bulk electric system Control Centers, and seeks comments on controls for transient electronic devices used on the bulk electric system.

Regarding supply chain management, recent malware campaigns targeting supply chain vendors highlight a gap in protection under the CIP Reliability Standards. In this new type of campaign, malware is injected into hardware or software components used for operations, or tools used to perform maintenance or other services on network components when in the control of a hardware, software or maintenance vendor, prior to delivery to a customer.

FERC is seeking comment on the proposal, what would constitute a reasonable time frame to address supply chain management, and the features of such a standard. The goal is a forward-looking, objective-driven standard that encompasses activities in the system development life cycle from research and development, design and manufacturing to acquisition, delivery, integration, operations, retirement and eventual disposal of the equipment and services.

The controls should accommodate differences among companies with regard to procurement, vendor relations, system requirements, information technology implementation and privileged commercial or financial information, using the National Institutes of Standards and Technology (NIST SP 800-161) as guidance. A standard pertaining to supply chain management security would:

- Address only the obligations of entities registered under FERC reliability rules;
- Be forward-looking and not require abrogation or renegotiation of contracts;
- Set goals about what to do while allowing flexibility for how an entity achieves those goals;
- Allow for exceptions given the diversity of acquisition processes; and
- Be specific enough so that compliance obligations are clear and enforceable.

Also today, FERC directed NERC to provide additional information as to why its Reliability Standards propose to limit risks posed by transient devices such as flash drives to only medium- and high-risk bulk electric service cyber systems. Omitting low-risk cyber systems from the standards could create a gap in protection, as malware inserted by a flash drive or laptop computer at a single low-impact substation could propagate through a network of many substations without encountering a single security control under NERC's proposal.

Comments on the proposal are due within 60 days of publication in the *Federal Register*.