



Federal Energy Regulatory Commission
July 16, 2015
Open Commission Meeting
Staff Presentation
Item E-1

"Good morning Mr. Chairman and Commissioners,

"Item E-1 is a draft Notice of Proposed Rulemaking that addresses proposed revisions to the Critical Infrastructure Protection or "CIP" Reliability Standards submitted by the North American Electric Reliability Corporation (NERC). NERC submitted the proposed revisions to the CIP Reliability Standards in response to the Commission's Order No. 791. The draft NOPR proposes to approve the proposed CIP Reliability Standards and find that they adequately address the directives in Order No. 791 by: (1) eliminating the "identify, assess, and correct" language in 17 of the CIP version 5 Standard requirements; (2) providing enhanced security controls for Low Impact assets; (3) providing controls to address the risks posed by transient electronic devices, such as thumb drives and laptop computers; and (4) addressing in an equally effective and efficient manner the need for a NERC Glossary definition for the term "communication networks."

"While the NOPR proposes to approve the CIP Standards, the NOPR raises several additional issues. First, while the NOPR proposes to find that NERC's modifications to provide protections for communication network components are adequate, the protections apply to a limited subset of control centers. The draft NOPR proposes to direct NERC to develop modifications to Reliability Standard CIP-006-6 to require protections for communication network components and data communicated between all bulk electric system Control Centers. Further, the draft NOPR seeks comment on the proposed scope of Reliability Standard CIP-010-2, which provides new security controls for transient electronic devices associated with High and Medium Impact BES Cyber Systems but does not address the risk to Low Impact BES Cyber Systems.

"In addition, the draft NOPR proposes to direct NERC to develop a new or modified Reliability Standard to provide security controls for supply chain management for industrial control system hardware, software, and computing and networking services associated with bulk electric system operations. As explained in the draft NOPR, changes in the bulk electric system cyber threat landscape identified through recent malware campaigns targeting supply chain vendors have highlighted a gap in the protections under the CIP Standards. This new type of malware campaign is based on the injection of malware while a product or service remains in the control of the hardware or software vendor, prior to delivery to the customer. The goal of the supply chain security controls should be to create a forward-looking, objective-driven standard that encompasses activities in the system development life cycle to support and ensure security, integrity, quality, and resilience of the supply chain and the future acquisition of products and services. The draft NOPR seeks comment on the proposal, including comment on a reasonable timeframe to implement new supply chain security controls.

"This concludes our presentation."