

Reliability and the Federal Energy Regulatory Commission

Michael Peters
Energy Infrastructure & Cyber Security Advisor
Federal Energy Regulatory Commission
202-502-8461
Michael.Peters@FERC.GOV

- The views expressed in this presentation do not represent the views of the Federal Energy Regulatory Commission or the United States.
- These views are the personal opinion of Mike Peters!!!! 😊 😊 😊

FERC Strategic Plan

- Goal 1: Energy Infrastructure – Promote the Development of a Strong Energy Infrastructure
 - Objective A: Stimulate Appropriate Infrastructure Development
 - Resolve regulatory and other challenges to needed development
 - Encourage investment and effect timely cost recovery
 - Objective B: Maintain a **Reliable** and Safe Infrastructure
 - **Assure reliability of interstate transmission grid**
 - Protect safety at LNG and hydropower facilities
 - Incorporate environmental considerations into Commission decisions

FERC Strategic Plan Continued

- Goal 2: Competitive Markets – Support Competitive Markets
- Goal 3: Enforcement – Prevent Market Manipulation

Federal Power Act (FPA)

Energy Policy Act of 2005 created Section 215 of Federal Power Act

'Reliability Standard'

Operation

Cybersecurity Protection

**Design of planned additions
or modifications**

§215(a) "(3) The term 'reliability standard' means a requirement, approved by the Commission under this section, to provide for reliable operation of the bulk-power system. The term includes requirements for the operation of existing bulk-power system facilities, including cybersecurity protection, and the design of planned additions or modifications to such facilities to the extent necessary to provide for reliable operation of the bulk-power system, but the term does not include any requirement to enlarge such facilities or to construct new transmission capacity or generation capacity."

FPA Continued

'Reliable operation'

Including a cybersecurity incident

§215(a) "(4) The term 'reliable operation' means operating the elements of the bulk-power system within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of such system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements."

FPA Continued

'Cybersecurity incident'

Disrupts

Attempt to disrupt

Devices

Communication networks

Hardware, software and data

§215(a) "(8) The term 'cybersecurity incident' means a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk-power system."

FPA Continued

is just, reasonable, not unduly discriminatory or preferential, and in the public interest

§215(d) "(2) The Commission may approve, by rule or order, a proposed reliability standard or modification to a reliability standard if it determines that the standard is just, reasonable, not unduly discriminatory or preferential, and in the public interest. The Commission shall give due weight to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed standard or modification to a reliability standard and to the technical expertise of a regional entity organized on an Interconnection-wide basis with respect to a reliability standard to be applicable within that Interconnection, but shall not defer with respect to the effect of a standard on competition. A proposed standard or modification shall take effect upon approval by the Commission."

FPA Continued

Upon its own motion or upon complaint

May order the Electric Reliability Organization to submit

Proposed reliability standard or a modification

To carry out this section

§ 215(d) "(5) The Commission, upon its own motion or upon complaint, may order the Electric Reliability Organization to submit to the Commission a proposed reliability standard or a modification to a reliability standard that addresses a specific matter if the Commission considers such a new or modified reliability standard appropriate to carry out this section."

Commission Process from 10,000 Feet

- Identify any concerns
- Find resolutions for concerns

The Process

- NERC submits the CIP-002 through CIP-009 to the commission
- FERC
 - Releases a preliminary staff assessment
 - Notice of Proposed Rulemaking
 - Final Rule – Order 706

Order 706

- Approved CIP-002 through CIP-009
 - However required major modifications to all 8 standards

Order 706 Major Modifications

- Removal of Reasonable Business Judgment
- Removal of Acceptance of Risk
- Technical Feasibility Exceptions still exist but greater structure required.
- Critical Asset Identification Oversight

Current Standard Drafting Team

- NERC & Industry have a CSDT 706 team currently working on modifications to the standards
- Phased approach
 - Phase 1 removal of reasonable business judgment & some other non-controversial “low hanging fruit”
 - Phase 2 – the bulk of the Order 706 directives
 - Phase 3 – very tough technical problems

Current Security Posture

- Varies Wildly dependent upon company
- General assessment is that much of the grid is vulnerable.
- FERC examined AURORA compliance
 - Only 7 of 30 companies had mitigated the vulnerability
 - Only 2 of 30 truly had a good cyber security posture.

Current Security Posture

- Implementation of CIPS should help
 - However Key is how the Critical assets are chosen
 - Fewer critical assets chosen means fewer cyber assets protected.
- Companies that “get it” working to secure all their cyber assets
- Companies that “don’t get it” just working to “comply”

Key Industry Education Moment

- COMPLIANCE DOES NOT EQUAL SECURITY!!!!
- Companies need to implement defense mechanisms so that they can safely, securely, and reliably operate the grid.

Future Efforts

- FERC will monitor the drafting team efforts.
- NIST standards may help
 - However, a good solid implementation of CIPS may provide more security than a poor implementation of NIST standards.
 - Key is whether companies “get it”.

Future Efforts

- FERC asking for additional authority
 - Advisories (AURORA, etc) voluntary
 - Need to be mandatory
 - Need to be able to direct defensive actions dependent upon threats & vulnerabilities.

Any Questions?