Supply Chain Risk Management Reliability Standard and Cyber Security Incident Reporting Notice of Proposed Rulemaking Update

---

Patricia Eke
Energy Industry Analyst
Office of Electric Reliability

June 7, 2018

Disclaimer

The views expressed herein are mine, and do not necessarily reflect the views of the Commission, individual Commissioners, Commission staff, or individual Commission staff members

Supply Chain Risk Management Reliability Standard (Order No. 829)

- Issued by the Commission: July 21, 2016
- Directs NERC to develop Reliability Standard(s) for supply chain risk management for industrial control system hardware, software, and computing and networking services associated with the Bulk-Power System
- Mitigate risk of a cybersecurity incident associated with reliable operations of the Bulk-Power System

FERC Order No. 829

In FERC Order No. 829, the Commission directed NERC to develop a Reliability Standard(s) to address supply chain risk management. The new or modified Standard should address the following security objectives:

1. Software Integrity and Authenticity
2. Vendor Remote Access
3. Information System Planning
4. Vendor Risk Management & Procurement Controls

FERC Order No. 829

- On September 26, 2017, NERC proposed new and enhanced Reliability Standards to address supply chain cybersecurity risk management as directed in Order No. 829:
  - CIP-013-1 (Cybersecurity- Supply Chain Risk Management Reliability Standards)
  - CIP-005-6 (Electronic Security Perimeter) and;
  - CIP-010-3 (Configuration Change Management)
- NERC Board of Trustees issued resolutions directing NERC to further study supply chain risks

FERC Order No. 829

- On January 18, 2018, the Commission proposed to adopt enhanced Supply Chain Risk Management Reliability Standards (SCRM)
- The Commission proposed to find that a significant cyber security risk remains in the proposed SCRM Standards and proposed to direct NERC to:
  - Include Electronic Access Control or Monitoring Systems (EACMS) associated with medium and high impact bulk electric systems within the scope of the SCRM Standards and;
  - Evaluate the risks presented by Physical Access Control Systems (PACS) and Protected Cyber Assets (PCA) as part of the study proposed by the NERC Board of Trustees

FERC Order No. 829

- Deadline for Comments: March 26, 2018
- Comments currently under Commission staff review

Cyber Security Incident Reporting Notice of Proposed Rulemaking (NOPR)

- Issued by the Commission: December 21, 2017
- Proposes to direct NERC to develop and submit modifications to the Critical Infrastructure Protection (CIP) Reliability Standards to improve the reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system

Cyber Security Incident Reporting NOPR

- Current reporting thresholds may understate the true scope of cyber-related threats facing the Bulk-Power System.

- Lack of any NERC reportable cybersecurity incidents in 2015 and 2016, suggests a gap in the current reporting requirements
  - DOE Electric Disturbance Reporting Form OE-417 contained four cybersecurity incidents reported in 2016: two suspected cyber attacks and two actual cyber attacks in 2016.
  - ICS-CERT responded to fifty-nine (59) cybersecurity incidents within the Energy Sector in 2016.

Cyber Security Incident Reporting NOPR Includes Five Proposals

1. Expanding the reporting threshold to include attempted compromise as well as actual compromise.
2. Specifying the content required in mandatory cyber security incident reporting.
3. Establishing a deadline for when the entity must file a cyber security incident report to E-ISAC.
4. Including DHS ICS-CERT as a mandatory recipient of these incident report.
5. Requiring that NERC file an annual, public, and anonymized summary of the cyber security incidents.

Cyber Security Incident Reporting NOPR

- Deadline for Comments: February 26, 2018
- Comments currently under Commission staff review

Questions?