NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Physical Security CIP-014-1

Industry Webinar
December 18, 2014

RELIABILITY | ACCOUNTABILITY




Agenda

- Federal Energy Regulatory Commission (FERC) Order Summary
- Standard Drafting Team (SDT) Activities
- Guidance Development Activities
- Implementation Timeline

FERC Order 802
November 20, 2014

- The FERC approved the standard and directed NERC to **remove the term "widespread"** from Reliability Standard CIP-014-1 or to propose modifications to the Reliability Standard that address FERC's concerns within 6 months of the effective date of the order.
- Paragraph 31: The Commission adopts the NOPR proposal in part and **directs NERC to remove the term "widespread" from Reliability Standard CIP-014-1 or, alternatively, to propose modifications to the Reliability Standard that address the Commission's concerns**. The differing views expressed in the comments validate the concern raised in the NOPR that the meaning of the term "widespread" is unclear and subject to interpretation.

FERC Order 802 - Widespread

- Paragraph 32: We stated in the March 7 Order that "the Reliability Standards that we are ordering today apply only to critical facilities that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System. We affirm the March 7 Order's statement that **"[m]ethodologies to determine these facilities should be based on objective analysis, technical expertise, and experienced judgment."**

FERC Order 802 – Informational Filing

- Directed NERC to make an **informational filing** addressing whether CIP-014-1 provides physical security for all "High Impact" control centers necessary for the reliable operation of the Bulk-Power System. FERC directed NERC to submit this filing within two years after the effective date of the standard.
- Paragraph 45: The March 7 Order stated that a "critical facility is one that, if rendered inoperable or damaged, could have a critical impact on the operation of the interconnection through instability, uncontrolled separation or cascading failures on the Bulk-Power System."

FERC Order 802 – Informational Filing *(Continued)*

- Paragraph 45 (*continued*): - The March 7 Order, while not mandating that a minimum number of facilities be deemed critical under the physical security Reliability Standards, explained that the **"Commission expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."**

FERC Order 802 – Informational Filing *(Continued)*

- Paragraph 57: The Commission adopts the NOPR proposal and directs NERC to **submit an informational filing that addresses whether there is a need for consistent treatment of "High Impact" control centers for cybersecurity and physical security purposes** through the development of Reliability Standards that afford physical protection to all "High Impact" control centers. The Commission, however, modifies the NOPR proposal and extends the due date for the informational filing to two years following the effective date of Reliability Standard CIP-014-1.

FERC Order 802 – Informational Filing *(Continued)*

- Paragraph 58: While we approve Reliability Standard CIP-014-1 in this final rule, including the Reliability Standard's treatment of control centers, the Commission, for the reasons set forth in the NOPR, finds that **NERC should assess whether all "High Impact" control centers should be protected under Reliability Standard CIP-014-1.** We recognize that NERC and applicable entities will be in a better position to provide this assessment after implementation of Reliability Standard CIP-014-1 and Reliability Standard CIP-006-5, the latter of which provides some physical protection to "High Impact" control centers. Accordingly, the Commission directs NERC to submit the informational filing two years following the effective date of Reliability Standard CIP-014-1.

FERC Order 802 – Informational Filing *(Continued)*

- Paragraph 58 (*continued*): The Commission, while not directing NERC to submit the informational filing as CEII, recognizes the concerns raised by commenters regarding confidentiality. **The Commission expects NERC to prepare the informational filing and submit it in such a way as to protect any critical information from public disclosure.**

FERC Order 802 – Informational Filing *(Continued)*

- Paragraph 59: At this time, the Commission will **not direct NERC to address in the informational filing whether all "High Impact" and "Medium Impact" BES Cyber Assets should be considered critical** for the purposes of Reliability Standard CIP-014, Requirement R1. We are sympathetic to several points raised in ITC's comments, which echo some of the statements in the NOPR. However, as stated in the NOPR, the basis for directing an informational filing regarding control centers is found in the March 7 Order, where the Commission stated that it "expects that critical facilities generally will include, but not be limited to, critical substations and critical control centers."

FERC Order 802 – Informational Filing *(Continued)*

- Paragraph 59 (*continued*): - While NERC explained why not all "High Impact" control centers may be critical for the purposes of Reliability Standard CIP-014-1, we **conclude that this issue requires close attention and should be addressed in the informational filing**. The broader concerns raised by ITC regarding the scope of Requirement R1 can be evaluated by NERC and industry as part of the implementation process.

FERC Order 802 – Informational Filing *(Continued)*

- 59 (*continued*): As we noted above, the Commission will devote resources to compliance with and enforcement of Reliability Standard CIP-014-1 to ensure that all critical facilities are identified pursuant to Requirement R1. **Should the Commission find through these efforts, or through the post-implementation reports and informational filing that NERC will submit, that Requirement R1 as currently written is not capturing all critical facilities, then the Commission will act upon that information.**

SDT Activities

- Revised SAR to address use of “widespread” was approved for posting by the NERC SC on December 9, 2014.
- SAR was posted for 30-day informal comment period (December 15, 2014-January 13, 2015).
- SDT will consider any comments received on the SAR and begin standard development process in January-February 2015.
- Due date for petition for approval of revisions to CIP-014 to address “widespread” directive - **July 27, 2015**.

Guidance Development Activities

- NERC will work with industry groups, such as NATF, to develop guidance. The guidance will address:
  - Best practices and effective approaches to meet each requirement
  - Compliance-oriented communication for common regional compliance and enforcement
- Stakeholder groups will be formed to field industry FAQs. The group will include:
  - Industry groups
  - Regional Compliance and Enforcement staff
  - NERC Committees
    - PC
    - CIPC

CIP-014-1 Guidance

- Transmission Owner to review Section 4 Applicability to determine whether or not the standard applies to them.
  - Applicability is based on CIP-002-5 Medium Impact facilities
- Applicable Transmission Owner to perform risk assessment and identify critical facilities on or before the effective date of CIP-014-1.
- Guidance for Requirement R1 risk assessment performance includes:
  - Guidelines and Technical Basis Section of CIP-014-1
  - NATF documentation
  - TPL-001-4, Requirements R4-R6
  - Other methods that meet the intent of the requirement to identify critical stations or substations.

CIP-014-1 Implementation

- Critical facility identification (R1) complete before effective date (six months following publication in the Federal Registry)
  - Standard approved November 20, 2014
  - **Mandatory and Enforceable October 1, 2015**
- Third party verification (R2) complete within 90 days of completion of R1:
  - **Mandatory and Enforceable no later than December 30, 2015**
  - **Part 2.3 - revisions to list could add 60 days**
- Notification of other parties (R3) complete within 7 days of completion of R2.

Implementation

- Evaluate threats and vulnerabilities (R4) and develop security plans (R5).
  - **Mandatory and Enforceable 120 days after completion of R2**
- Third party review of threats and vulnerabilities and security plans (R6).
  - **Mandatory and Enforceable 90 days after completion of R4/R5**
  - **Part 6.3 – revisions to threats, vulnerabilities and plans could add 60 days**

CIP-014-1 Implementation Timeline

	Publish Guidance	Earliest Mandatory Enforcement
R1, R2 & R3 Risk Assessment & Verification Guidance Review NATF Guidance (R1) and provide any substantive edits Develop Compliance and Enforcement Letter to the ERO (R1, R2, R3)	January 2015	Oct 1, 2015
R4 & R5 Threat Evaluation / Physical Security Plans Develop Compliance and Enforcement Letter to the ERO (R4, R5)	April 2015	May 1, 2016
R6 Physical Security Plan Verifications Develop Compliance and Enforcement Letter to the ERO (R6)	July 2015	Aug 1, 2016

ERO to Monitor Implementation

- Number of assets critical under the standard
- Defining characteristics of the assets identified as critical
- Scope of security plans (types of security and resiliency contemplated)
- Timelines included for implementing security and resiliency measures
- Industry's progress in implementing the standard

Information

- NERC Standards Developer, Stephen Crutchfield
- NERC CIP Compliance Manager, Tobias Whitney
  - Email: stephen.crutchfield@nerc.net or tobias.whitney@nerc.net
  - Project Page: http://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx
  - CIP-014-1 Standard: http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-014-1&title=Physical%20Security&jurisdiction=United%20States

Questions