NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Physical Security Reliability Standard

Physical Security Technical Conference
Atlanta, Georgia
April 1, 2014

RELIABILITY | ACCOUNTABILITY



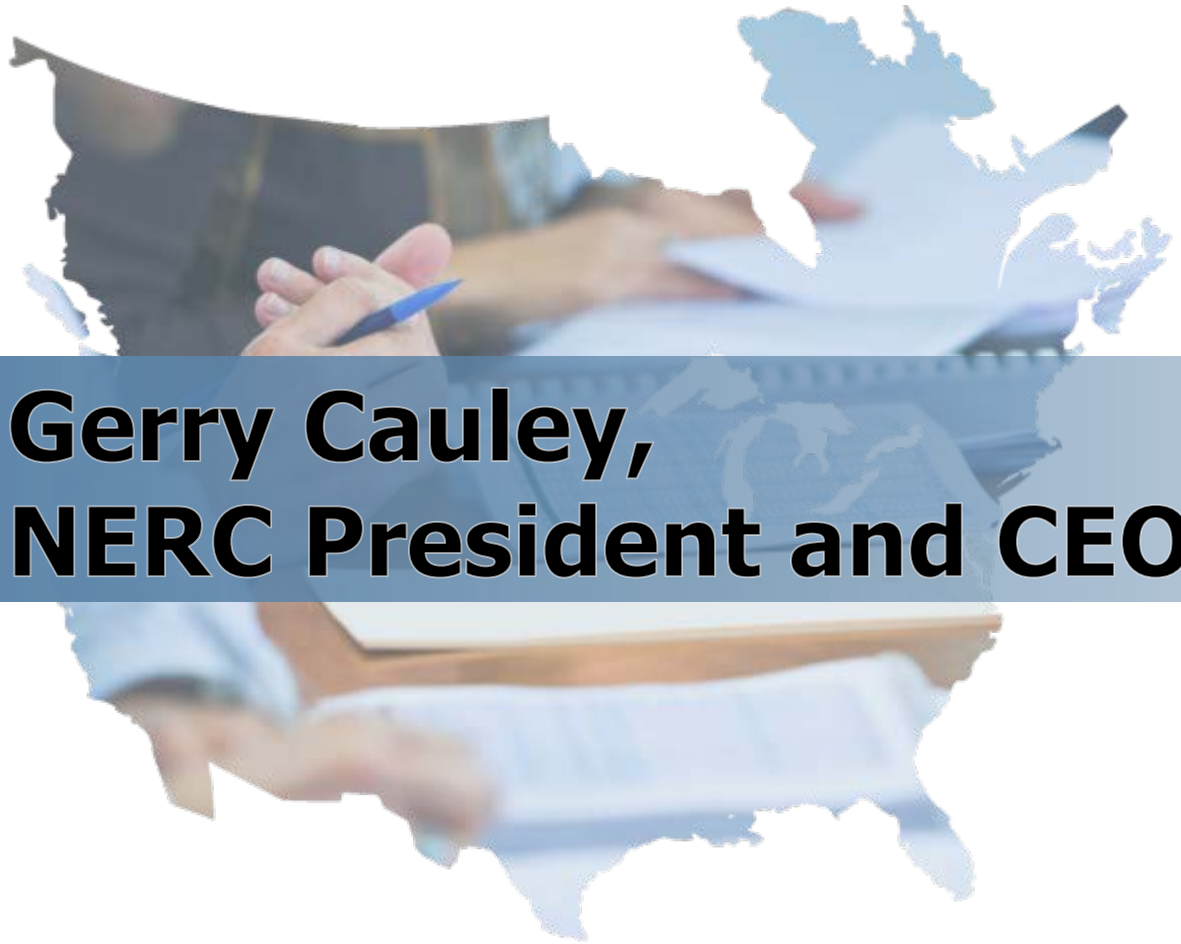

Agenda

- NERC Antitrust Compliance Guidelines and Public Announcement
- Introductions and Opening Remarks
- Review conference objectives and ground rules
- Update on standards development process
- Review Federal Energy Regulatory Commission (FERC) Order on Physical Security
- Review and discuss draft standard
- Overview of Compliance Reliability Standard Audit Worksheet (RSAW) approach
- Review action plan and milestones

NERC Antitrust Compliance Guidelines and Public Announcement

- It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition. It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.
- Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

Introductory Remarks



Gerry Cauley, NERC President and CEO

Susan Ivey, Exelon Utilities
Standard Drafting Team Chair

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Standard Drafting Team

Name	Entity
Susan Ivey (Chair)	Exelon Corporation
Lou Oberski (Vice Chair)	Dominion
John Breckenridge	Kansas City Power & Light
Ross Johnson	Capital Power
Kathleen Judge	National Grid
Mike O'Neil	Florida Power & Light / NextEra, Inc.
Stephen Pelcher	Santee Cooper
John Pespisa	Southern California Edison
Robert Rhodes	Southwest Power Pool
Allan Wick	Tri-State Generation and Transmission
Manho Yeung	Pacific Gas and Electric Company

Conference Objectives

- Collect information and stakeholder perspectives for the Standard Drafting Team (SDT) to support standard development
- Discuss key issues and directives in the FERC Order on Physical Security
- Inform stakeholders on the proposed action plan

Ground Rules

- No confidential, non-public information will be discussed
- Focus is on guidance to assist SDT
  - Comments should focus on recommendations and solutions for drafting a physical security standard
- Follow a facilitation format for broad participation

Discussion Topics

- Applicability of the standard
- Risk assessment to identify critical facilities
- Evaluation of potential threats
- Physical security plans
- Compliance RSAW approach

Format

- NERC staff will present each topic, including
  - Relevant section of the FERC Order
  - Requirement language from the draft standard
- SDT leaders may provide some initial considerations
- Opportunity for participant input and discussion
  - In-person participants use microphones and identify yourself and your organization
  - Remote participants provide input by chat
- Facilitator will recap themes
- Opportunity for SDT members to ask clarifying questions

Standards Development Update

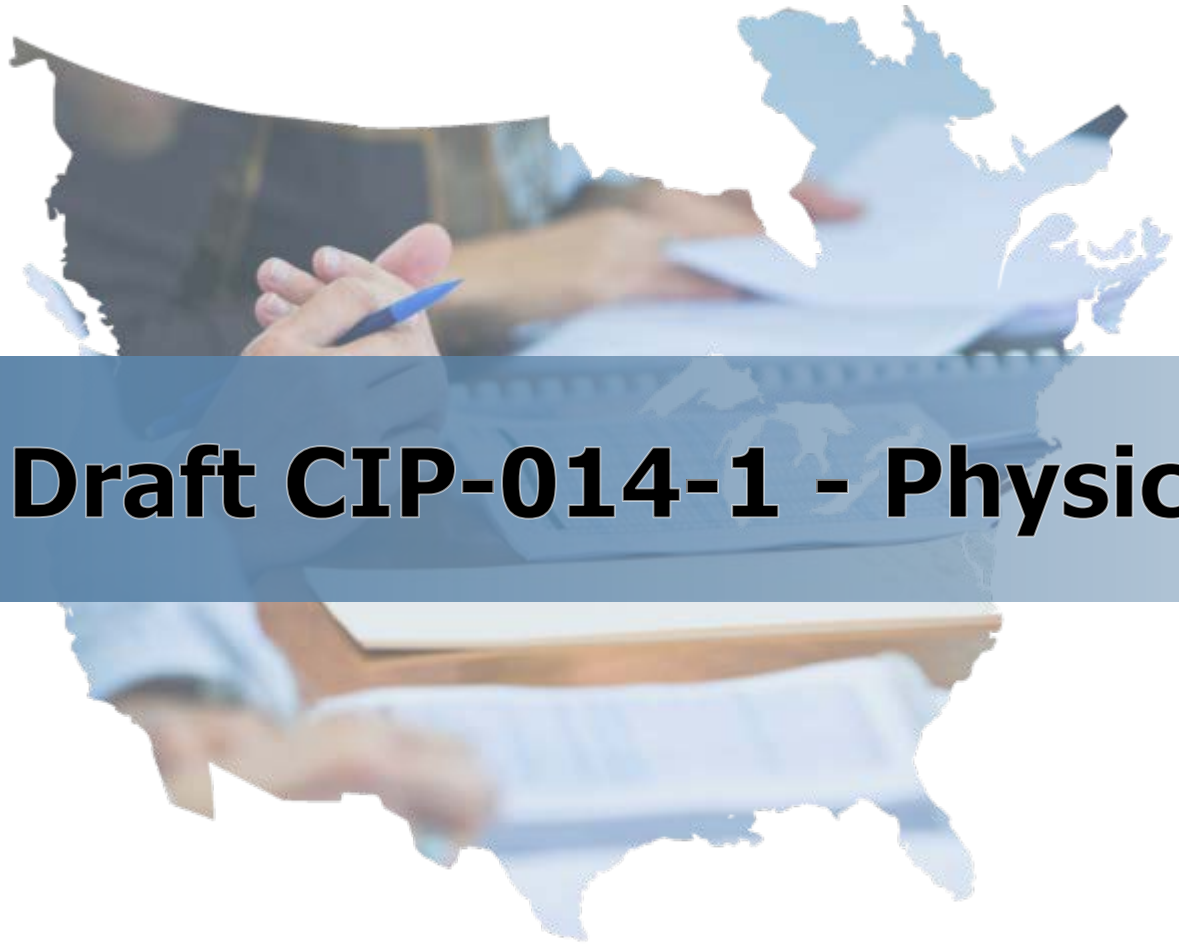
- March 7, 2014: FERC Order (RD14-6)
- March 13–18, 2014: SDT nomination period
- March 21, 2014: Standards Committee action
  - Accepted the Standard Authorization Request (SAR)
  - Appointed the SDT
  - Authorized waiver of certain provisions of the Standard Process Manual necessary to meet regulatory deadline
- March 22–28, 2014: SAR posted for informal comment
- SDT meeting April 2-4, 2014

Project Page:
http://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx

FERC Order

FERC Order on Physical Security

- NERC is directed to file Reliability Standard(s) to address physical security risks to the Bulk Power System (BPS) by June 5, 2014
- The standards should require owners and operators to address risks of physical attack on BPS reliability in three steps:
  - Identify critical facilities (P.6)
  - Evaluate potential threats and vulnerabilities to critical facilities (P.8)
  - Develop and implement a security plan to protect against identified threats (P.9)
- Require owners and operators to periodically reevaluate all steps for continued effectiveness (P.12)



Draft CIP-014-1 - Physical Security

Purpose

- "To identify and protect transmission substations and their associated primary Control Centers that, if rendered inoperable or damaged as a result of a physical attack, could result in instability, uncontrolled separation, or Cascading within an Interconnection."
- Drafted as Critical Infrastructure Protection (CIP) family of standards

Applicability

Draft Standard

- **Applicability** includes those functional entities with facilities that may have a critical impact as result of physical attack
- CIP-002-5 Medium impact rating criteria for transmission facilities provides an existing framework

Order

- Include facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading (P.6)
- Generally include critical substations and critical control centers (Fn.6)

Applicability

- Transmission Owner (TO) that owns any of the following Transmission Facilities (CIP-005-2 Medium impact criteria):
  - Operated at 500 kV or higher
  - Operating between 200 kV and 499 kV and meeting the “aggregate weighted value” criteria (see table)
  - Critical to the derivation of Interconnection Reliability Operating Limits (IROL) and their associated contingencies
  - Essential to meeting Nuclear Plant Interface Requirements
- Transmission Operator (TOP)
- Exemption for nuclear facilities under an approved plan

Identify Critical Facilities

Draft Standard

- **Requirement R1** requires the TO perform a risk assessment through transmission analysis to identify:
  - Each transmission substation (existing and planned) that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading within an Interconnection
  - Associated control centers

Order

- Include facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading (P.6)
- Generally include critical substations and critical control centers (Fn.6)

Identify Critical Facilities

Draft Standard

- **Requirement R1** specifies that the assessment shall be conducted at least once every 30 months
  - Identification of critical-impact facilities is appropriate for the Near-term Planning Horizon

Order

- Require the identification of critical facilities to be periodically reevaluated (P.11)

Identify Critical Facilities

Draft Standard

- **Requirement R2** requires the TO notify the TOP that operates the primary Control Center identified in Requirement R1
  - In circumstances where the TO does not control of the identified Control Center, this notification is necessary for the TOP to fulfill security plan requirements

Order

- Include facilities that, if rendered inoperable or damaged, could result in instability, uncontrolled separation, or cascading (P.6)
- Generally include critical substations and critical control centers (Fn.6)

Identify Critical Facilities

Draft Standard

- **Requirement R3** requires the TO obtain verification of the risk assessment within 90 days of completion
  - TO must select a registered Planning Coordinator (PC), Transmission Planner (TP), Reliability Coordinator (RC); or an entity with transmission planning or analysis experience

Order

- An entity other than the owner or operator is required to verify the risk assessment (P.11)

Identify Critical Facilities

Draft Standard

- **Requirement R3** also requires the TO act on recommendations by the verifying entity to add or remove facilities by:
  - Modifying its identified facilities, or
  - Documenting the technical basis for not modifying its identified facilities

Order

- Include a procedure for adding or removing facilities as a result of verification (P.11)

Identify Critical Facilities

Draft Standard

- **Requirement R3** also requires the TO implement procedures for protecting sensitive or confidential information exchanged with the verifying entity
  - Non-disclosure agreements and procedures to prohibit removal of information are examples

Order

- Include provision for confidential treatment of sensitive information (P.10)

Evaluate Potential Threats

Draft Standard

- **Requirement R4** requires the TO and TOP of identified facilities to conduct an evaluation of potential physical threats and vulnerabilities
  - Evaluation must consider any unique characteristics of the facility and the type of physical attack that can be realistically contemplated

Order

- Require tailored evaluation of physical threats and vulnerabilities (P.8)
- Consider characteristics of the facility and the type of attacks that can be realistically contemplated (P.8)

Implement Security Plans

Draft Standard

- **Requirement R5** requires the TO and TOP develop and implement a documented security plan covering each identified facility

Order

- Require owners and operators of identified facilities to develop and implement a security plan to address evaluated threats (P.9)

Implement Security Plans

Draft Standard

- Security plans must include the following attributes:
  - Identification of measures to deter, protect, and detect physical threats
  - Response plan with law enforcement contacts
  - Timeline for implementation
  - Provisions to reevaluate evolving physical threats

Order

- Require owners and operators of identified facilities to develop and implement a security plan to address evaluated threats (P.9)

Implement Security Plans

Draft Standard

- **Requirement R6** requires the TO and TOP obtain a review of the threat evaluation (Requirement R4) and security plan (Requirement R5)
  - TO/TOP shall select a reviewing entity with Certified Protection Professional (CPP) or Physical Security Professional (PSP) certified staff

Order

- The evaluation of potential threats and security plan must be reviewed by an entity with appropriate expertise (P.11)

Implement Security Plans

Draft Standard

- **Requirement R6** also requires the TO and TOP act on recommendations from the reviewing entity by:
  - Modifying its security plan, or
  - Documenting the technical basis for not modifying its security plan

Order

- The evaluation of potential threats and security plan must be reviewed by an entity with appropriate expertise (P.11)

Implement Security Plans

Draft Standard

- **Requirement R6** also requires the TO and TOP implement procedures for protecting sensitive or confidential information exchanged with the reviewing entity
  - Non-disclosure agreements and procedures to prohibit removal of information are examples

Order

- Include provision for confidential treatment of sensitive information (P.10)

CIP-014-1 Implementation Plan

Draft Standard

- Requirements to identify facilities (R1, R2, and R3) proposed to become effective six-months after regulatory approval
- Requirements to evaluate threats and implement security plans (R4, R5, and R6) proposed to become effective 12-months after regulatory approval

Order

- Implementation plan should include timeframes for completing the steps required by the Order (Fn.8)

CIP-014-1 RSAW Development

- RSAW team will provide an RSAW for concurrent posting with the CIP-014-1 standard
  - RSAW team consists of 12 members from NERC and the Regional Entities
- Team members attend technical conference and SDT meetings
  - RSAW is reviewed with the SDT prior to posting
- Industry can comment on the RSAW after it is posted

Overview of Next Steps

- SDT meeting April 2-4, 2014
- Draft standard posted for 15-day initial comment and 5-day ballot mid-April
  - Standards Committee authorized waiver
- Industry webinar during initial comment and ballot
- SDT meeting end of April
  - Review and respond to comments
  - Revise the draft standard, implementation plan, and supporting material as necessary
- Revised standard posted in early May (as determined by initial comment and ballot period)
- Board of Trustees adoption and filing by June 5, 2014

Questions and Answers

Project Page:
http://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx