Morgan Lewis

Understanding NERC's New Physical Security Standard

Stephen M. Spina
J. Daniel Skees

June 10, 2014 at 1 pm Eastern

Instructions

- The audio will remain quiet until we begin. We will give periodic stand-bys until we are ready to begin at 1:00 p.m. (ET).
  - Audio is available via **Audio Broadcast**; you will hear the audio through your computer speakers. Please do **NOT** close the Audio Broadcast window.
    - **Make sure your speakers are ON and UNMUTED**
    - **Make sure your volume is turned up for the event**
- ONLY for attendees that are not able to hear audio through their computer speakers, you may join the teleconference. To do this, please:
  - Call-in toll-free number (US/Canada): 1-866-469-3239
  - Tech Support: If you are experiencing issues with your audio broadcasting, please call 866-229-3239.
    - This event is listen only. Please use the Q&A tab to communicate with the presenters.

Agenda

- Background
- Applicable Entities
- Identifying Critical Facilities
- Performing Threat Evaluations
- Developing a Security Plan
- Implementing the Standard
- Enforcement Expectations
- Protecting Sensitive Information
- Questions

Background

- Political pressure & media attention
- FERC's March 2014 order directs new Standard:
  1) Major Components
     1) Risk assessments to identify critical facilities
     2) Threat evaluations for identified facilities
     3) Develop and implement a security plan
  2) Minor Components
     1) Protect sensitive information
     2) Third-party verification for identified facilities
     3) Third-party review of identified threats and security plan
- Short, 90-day turnaround imposed
- CIP-014-1 filed with FERC on May 23, 2014

Applicable Entities

- The Standard will apply to you if you are a Transmission Owner of transmission facilities:
  - 500 kV + or 200 kV to 499 kV substation connected to 3+ substations and with an aggregate weighted value above 3000
  - Critical to derivation of an IROL
  - Part of a Nuclear Power Interface Requirement

  Note: This only means you must do the initial criticality analysis
- Transmission Operators for identified critical facilities
  - Usually the same as the Transmission Owner, but not in all instances
- Key concern: Joint ownership

Identifying Critical Facilities

- Requirement R1: Risk assessment of applicable facilities to determine what would happen if those facilities were "rendered inoperable or damaged."
  - Would it result in "widespread instability, uncontrolled separation, or cascading"?
- Requirement R2: Must be verified by an unaffiliated third party that is a PC, TP, or RC, or otherwise has transmission planning or analysis experience
  - Third-party may recommend that facilities be added or dropped
  - TO must adopt recommendation or document technical basis for disagreement
- Requirement R3: If TO has critical facilities, must notify applicable TOPs

Performing Threat Evaluations

- Requirement R4: Evaluate potential physical threats to and physical vulnerabilities of critical facilities
  - Consider any unique characteristics
  - Consider history of attacks on facilities of that type
  - Consider warnings from ES-ISAC, law enforcement, intelligence agencies
- Requirement R6: Unaffiliated third party must review vulnerability analysis
  - If third party recommends changes to vulnerability analysis, must adopt those changes or document reason for disagreement

Developing a Security Plan

- Requirement R5: Develop and implement a security plan
  - "Deter, detect, delay, assess, communicate, and respond to" the identified threats and vulnerabilities
  - Provide for contact and coordination with law enforcement
  - Include a timeline for any physical security enhancements
    - Must implement enhancements consistent with timeline
  - Address evolving security threats
- Requirement R6: Third-party review of security plan
  - Reviewer must fall within certain categories of physical security expertise in the Standard
  - If changes to plan are recommended, plan must be modified or must document reason for disagreement

Implementing the Standard

- Effective date is first day or first calendar quarter six months after FERC approval.
  - Requirement R1 risk assessment must be performed prior to effective date
  - Other Requirements cascade following effective date
    - 90 days for third-party verification
    - If no changes from third-party verification, 120 days to perform threat and vulnerability assessment and develop security plan
    - 90 days after threat assessment and security plan complete for third-party verification to occur

Enforcement Expectations

- Politically charged issue
- Surveys
- CMEP Tools
  - Audits
  - Spot checks
  - Data collection
  - Self-certifications
- Confidentiality limitations = More in-person reviews and physical inspections

Protecting Sensitive Information

- Every requirement involving third-party reviews and verifications also requires that confidentiality protections be in place to address handling of sensitive information by unaffiliated entity
- Likely challenges in NDAs:
  - Consultant specific vs. Registered Entity specific
  - Handling of information during review
  - Handling/disposal of information after review
  - Improper disclosure remedies
  - Government and discovery requests
  - Use of information by third-party
  - Audits by Regional Entities

Questions?

- Contact Information:

  Stephen M. Spina

  sspina@morganlewis.com

  202-739-5958

- J. Daniel Skees

  dskees@morganlewis.com

  202-739-5834

DISCLAIMER

- This material is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It does not constitute, and should not be construed as, legal advice on any specific matter, nor does it create an attorney-client relationship. You should not act or refrain from acting on the basis of this information. This material may be considered Attorney Advertising in some states. Any prior results discussed in the material do not guarantee similar outcomes. Links provided from outside sources are subject to expiration or change.

- **IRS Circular 230 Disclosure**
To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing, or recommending to another party any transaction or matter addressed herein. For information about why we are required to include this legend, please see http://www.morganlewis.com/circular230.

Morgan Lewis