2018 EEI/AGA Chief Audit Executives Conference

NERC standards

13 June 2018
Poll

What kind of organization is the North American Electric Reliability Corporation (NERC)?

A. Shareholder corporation
B. Non-profit
C. Privately held corporation
D. Government entity
E. None of the above
NERC
Establishment in current role

► The 2003 Northeast blackout led to regulatory reforms specified in Section 215 of the Federal Power Act of 2005
► Section 215 required the establishment of an Electric Reliability Organization (ERO)
► Federal Energy Regulatory Commission (FERC) designated NERC as the ERO
► Department of Energy (DOE) designated NERC as the Electricity Information Sharing and Analysis Center (E-ISAC)
NERC
Functional duties and oversight

➢ To ensure the reliability of the Bulk-Power System in North America
  ➢ Develops and enforces Reliability Standards
  ➢ Annually assesses seasonal and long-term reliability
  ➢ Monitors the Bulk-Power System
  ➢ Educates, trains, and certifies industry personnel

➢ Subject to oversight by the Federal Energy Regulatory Commission in the United States
NERC Regions

CIP-003-7
Low impact revisions

► Revisions completed in response to directives in FERC Order 822
► Eliminated “LERC” and “LEAP” definitions
  ► Embedded concepts directly into requirement language
  ► Updated reference diagrams
► Added Transient Cyber Asset (TCA) for low impact Bulk Electric System (BES) Cyber Systems
► The new standard pushes compliance for Sections 2, 3, and 5 out to January 1, 2020
CIP-003-7
Low impact revisions

► Uses the phrase “asset containing Low Impact BES Cyber Systems”
  ► This means the station, plant, or Control Center that contains the BES Cyber Systems
  ► Physical and cyber security requirements apply to the group of BES Cyber Systems as a whole, generally implemented as border protections around them
  ► Does not require a discrete list of BES Cyber Systems (but does require a list of “assets containing low impact BES Cyber Systems”)
► Continues to focus protections on “routable communications”
Ten reference diagrams

- Modified in response to FERC’s concerns dealing with “direct” communications (as compared to indirect communications)
  - Eliminated references to “direct” communications
- All show routable communications crossing the “asset boundary”
  - Not all show routable communication to low impact BES Cyber Systems
- No reference diagrams for serial-only communications
CIP-003-7
Transient cyber assets and removable media

- Modified definitions to include low impact environment concepts
- Added new “Section 5” to Attachments 1 and 2
  - Consistent with keeping all (cyber security protection) requirements for low impact BES Cyber Systems continue to reside in CIP-003
- TCA language is modeled after and consistent with TCA language in CIP-010
  - Allows consistent programs for all TCAs, if desired
  - Eliminated sections which imply “inventory”
Supply chain

- FERC initiated through technical conference on supply chain, followed by an order for a new standard
- Creates one new standard (CIP-013-1) and modifies two existing standards (CIP-005-6 and CIP-010-3)
- Approaches the threats from supply chain through technical and procedural controls
Supply chain
CIP-013-1

- Requires a plan for the procurement of BES Cyber Systems that addresses cyber security risks
  - Plan should consider both hardware and software
  - Notification and response to vendor-identified cyber security incidents
  - Notification for vendor personnel access management
  - Vendor disclosure of known vulnerabilities
  - Vendor enablement of software integrity and authenticity verification
  - Management of vendor remote access (includes system-to-system)
Supply chain
CIP-013-1

► Implement the plan
  ► Does not require renegotiation or abrogation of existing contracts
  ► The actual terms and conditions of a procurement contract are out of scope
  ► Vendor performance and adherence to a contract are out of scope
Supply chain
CIP-005-6

► Be capable of determining active vendor remote access sessions
  ► Interactive Remote Access
  ► System-to-System remote access
► Be capable of disabling vendor remote access sessions
Before making a change to the baseline that impacts:
- Operating system or firmware
- Commercially available or open-source software
- Security patches

Verify the identity of the source
Verify the integrity of the software

Only required if the method to verify the identity and integrity are available
Natural gas and electricity generation

- As of 2017 natural gas has overtaken coal as the largest source of electric generation: 31.7% vs. 30.1%*
- Unlike coal which can be stockpiled, natural gas is mostly on-demand delivery
- Much like electricity, natural gas delivery systems are vulnerable to disruptions
- Electric power generation dependency on natural gas is raising its profile:
  - NERC’s GridEx IV exercise notes fuel diversity (or the lack thereof) as common-mode vulnerability
- Cyber Assets supporting gas handling systems at generating plants may be considered BES Cyber Assets

Contact

Josh Sandler
Manager, Risk
Joshua.Sandler@ey.com
+1 765 404 8253
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2018 Ernst & Young LLP.
All Rights Reserved.

1805-2712004
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com