FORWARD TOGETHER RELIABILITYFIRST

CIP STANDARDS FOR LOW IMPACT GO/GOP ENTITIES- 101

Shon Austin, Principal Technical Auditor

RF Tech Talk, May 20, 2024

RELIABILITY FIRST

O B J E C T I V E

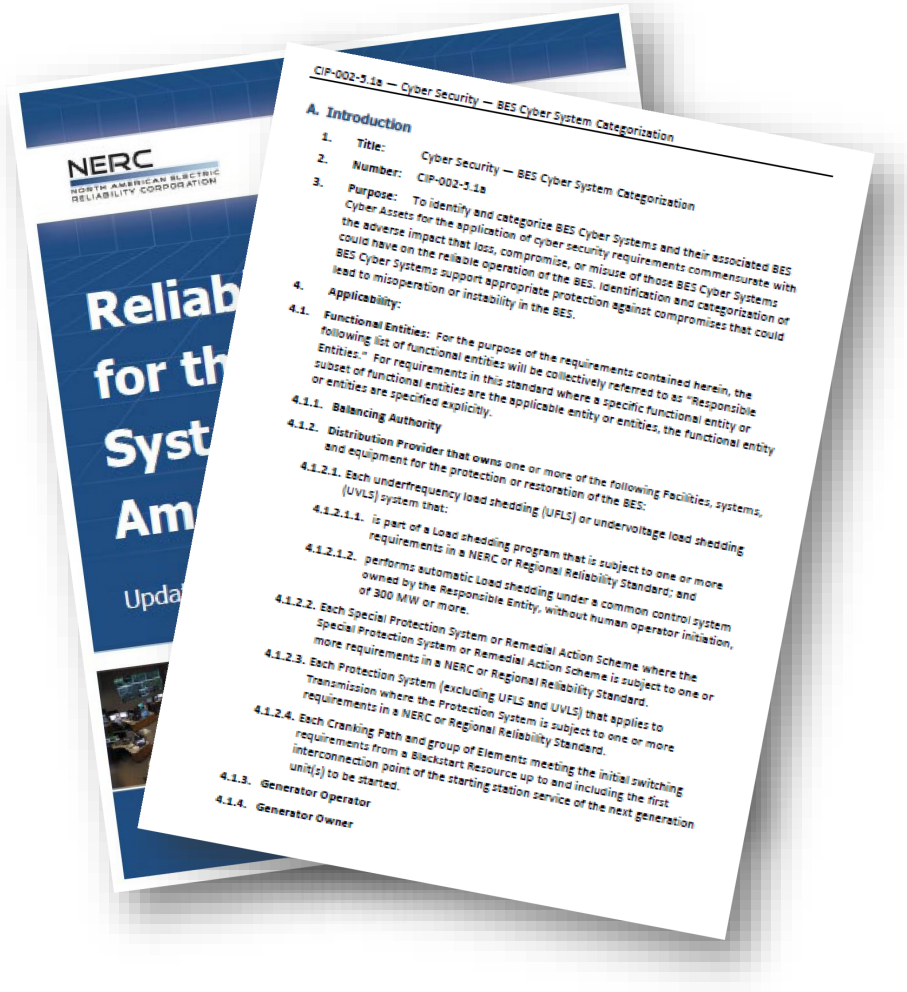
This presentation serves as a comprehensive desktop reference guide, offering valuable insights and resources pertaining to CIP-002-5.1a and CIP-003-8 processes

AGENDA

- LOW IMPACT DETERMINATION
- CIP-002-5.1A:
  - Background and information pertaining to Standard
- CIP-003-8:
  - Background and information pertaining to Standard
- INTERNAL CONTROLS: TYPES OF INTERNAL CONTROLS

LOW IMPACT DETERMINATION

- Categorization Criteria (CIP-002)
  - Requirement R1 only requires the discrete identification of BES Cyber Systems for those in the High Impact and Medium Impact categories.
  - All BES Cyber Systems for assets **not** included in **Attachment 1 –Impact Rating Criteria, Section 1 or Section 2, and listed in Section 3,** default to **Low Impact.**



CIP-002-5.1

- An implemented Process that considers each of the following assets for parts 1.1 through 1.3:
  - Control Centers and Backup Control Centers, Transmission Stations and Substations, Generation Resources, Systems and Facilities Critical to System Restoration (Blackstart Resources and Cranking Paths), Remedial Action Schemes that support the reliable operation of the BES and For Distribution Providers, Protection Systems specified in Applicability Section 4.2.1.
- P1.3 - Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).
- Evidence that the identifications in R1 and its parts (and update them if there are changes identified) have been reviewed at least once every 15 calendar months, even if there are no identified items in R1.
- Evidence that the CIP Senior Manager or delegate has approved the identifications required by R1 at least once every 15 calendar months, even if there are no identified items in R1.

Evidence Request Tool Reference

Request ID	Standard & Requirement
CIP-002-R1-L1-01	CIP-002 R1
CIP-002-R1-L1-02	CIP-002 R1
CIP-002-R1-L1-03	CIP-002 R1
CIP-002-R1-L1-04	CIP-002 R1
CIP-002-R1-L1-05	CIP-002 R1
CIP-002-R1-L1-06	CIP-002 R1
CIP-002-R1-L1-07	CIP-002 R1
CIP-002-R1-L1-08	CIP-002 R1
CIP-002-R1-L1-09	CIP-002 R1
CIP-002-R2-L1-01	CIP-002 R2 Part 2.1 R2 Part 2.2

CIP-003-8 R1 & R2

- R1: Cyber Security Policies for the following:
  - Cyber Security Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Cyber Security Incident Response
  - Transient Cyber Assets and Removable Media Malicious Code
  - Declaring and Responding to CIP Exceptional Circumstances

Evidence Request Tool Reference	
Request ID	**Standard & Requirement**
CIP-003-R1-L1-01	CIP-003 R1
CIP-003-R2-L1-01	CIP-003 R2

- R2: Cyber Security Plans (and supporting evidence) for Low Impact BES Cyber Systems (BCS) that Include the Sections 1-5 in Attachment 1
  - Each of the Sections in Attachment 1 provide additional detail for what each Low Impact Entity needs to have in place to meet the requirement
  - R2 is the heavy lift for Low Impact Entities due to the number of additional "Requirements" listed in Attachment 1, Sections 1-5

CIP-003 R2 ATTACHMENT 1

- Section 1 – Cyber Security Awareness
  - Reinforce cybersecurity practices every 15 calendar months
- Section 2 – Physical Security Controls
  - Each Responsible Entity shall control physical access, based on need
- Section 3 – Electronic Access Controls
  - Permit only necessary inbound and outbound electronic access
  - Authenticate all Dial-up Connectivity, if any
- Section 4 – Cyber Security Incident Response
  - Identification, Classification and Response, Reportable, Roles and Responsibilities, Incident Handling, Testing at least every 36 calendar months, Updating process within 180 days after test or actual Incident
- Section 5 - Transient Cyber Asset and Removable Media Malicious Code Risk Mitigation
  - Managed by the Responsible Entity – Method to mitigate the introduction of malicious code
  - Managed by a party other than the Responsible Entity – Method used to reduce the risk of malicious code introduction
  - Removable Media - Method(s) to detect malicious code on Removable Media & Mitigation strategy

Evidence Request Tool Reference

Request ID	Standard & Requirement
CIP-003-R2-L1-02	CIP-003 R2 Sect 1
CIP-003-R2-L1-03	CIP-003 R2 Sect 4.4
CIP-003-R2-L1-04	CIP-003 R2 Sect 4.5
CIP-003-R2-L1-05	CIP-003 R2 Sect 4.6
CIP-003-R2-L2-01	CIP-003 R2 Sect 2
CIP-003-R2-L2-02	CIP-003 R2 Sect 3.1
CIP-003-R2-L2-03	CIP-003 R2 Sect 3.2
CIP-003-R2-L2-04	CIP-003 R2 Sect 4.2
CIP-003-R2-L2-05	CIP-003 R2 Sect 5.1
CIP-003-R2-L2-06	CIP-003 R2 Sect 5.2
CIP-003-R2-L2-07	CIP-003 R2 Sect 5.3

CIP-003 R2 ATTACHMENT 1

- Emphasis by the Compliance Team will be the detailed review of:
  - Remote Access

  Note: With the majority of Entities using contracted vendors to support their systems, it is vital that the interaction between the vendor and the Entity be highly secure.

- Be able to provide the following to the Compliance Team:
  - Network Diagram(s) showing how the vendor accesses the Entity systems through their network architecture
  - Firewall / Router Ruleset(s) and Configuration(s)
  - Any other security controls in place

CIP-003 R3 & R4

- R3. Each Responsible Entity shall identify a CIP Senior Manager by name and document any change within 30 calendar days of the change.

- R4. The Responsible Entity shall implement a documented process to delegate authority, unless no delegations are used. Where allowed by the CIP Standards, the CIP Senior Manager may delegate authority for specific actions to a delegate or delegates.

Evidence Request Tool Reference

Request ID	Standard & Requirement
CIP-003-R3-L1-01	CIP-003 R3
CIP-003-R4-L1-01	CIP-003 R4

INTERNAL CONTROLS

- Preventative Controls
  - Preventative controls aim to reduce the risk of a negative event occurring. Preventative controls can be physical or administrative controls depending on the requirement and capabilities at the entity's disposal.
    - Badge readers on a Control Center door are a physical preventative control, since they prevent unauthorized physical access into the Control Center. Common administrative preventative controls are procedures, checklists and training.
- Detective Controls
  - Detective controls seek to identify an issue that is occurring or has occurred.
  - Entity could establish alarms to alert system administrators if the physical access control system detects a door has been opened without a corresponding approved access card. In other words, the alarm detects and alerts personnel to a change from normal operations.
- Corrective Controls
  - Corrective controls correct issues once they have occurred.
    - Corrective controls return a situation to its normal state. Corrective controls can also be more compliance oriented. If a detective control identifies a potential noncompliance (PNC), the entity can remediate the issue and file a Self-Report.
- Testing Internal Controls
  - Once an entity has implemented internal controls, they can test the controls to verify that they are performing as expected. In a sense, testing controls is a control for the controls.