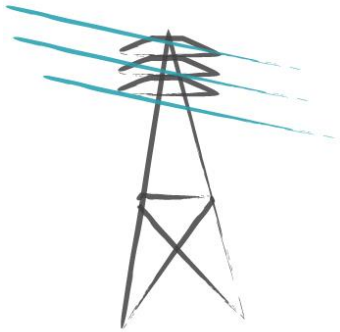


WECC

Decommissioning Assets & CIP

Holly Eddy, Compliance Auditor, Cyber Security

Eric Weston, Compliance Auditor, Cyber Security

Compliance Workshop November 14, 2017

Agenda

- Impact to Reliability
- Background
- Example Exercises
- Review CIP-011-2 R2
- Expectations at Audit

Impact to Reliability

Ensure entities are aware of requirements applicable to decommissioning as well as audit expectations of evidence for decommissioned assets (and why that evidence should be retained)

Background

- Each CIP Reliability Standard's *Compliance* Section 1.2 *Evidence Retention* states:

1.2. Evidence Retention:

The following evidence retention periods identify the period of time an entity is required to retain specific evidence to demonstrate compliance. For instances where the evidence retention period specified below is shorter than the time since the last audit, the CEA may ask an entity to provide other evidence to show that it was compliant for the full time period since the last audit.

The Responsible Entity shall keep data or evidence to show compliance as identified below unless directed by its CEA to retain specific evidence for a longer period of time as part of an investigation:

- Each Responsible Entity shall retain evidence of each requirement in this standard for three calendar years.
- If a Responsible Entity is found non-compliant, it shall keep information related to the non-compliance until mitigation is complete and approved or for the time specified above, whichever is longer.
- The CEA shall keep the last audit records and all requested and submitted subsequent audit records.

Exercise #1:
BCA associated with 230kV OCB

- Scenario:
  - PCB w/ digital relays
  - Medium Impact BCS without ERC
- Redeploy? Disposal?
  - CIP-011-2 R2
- Update CIP-002 R1 lists?
  - Discrete lists of devices not required

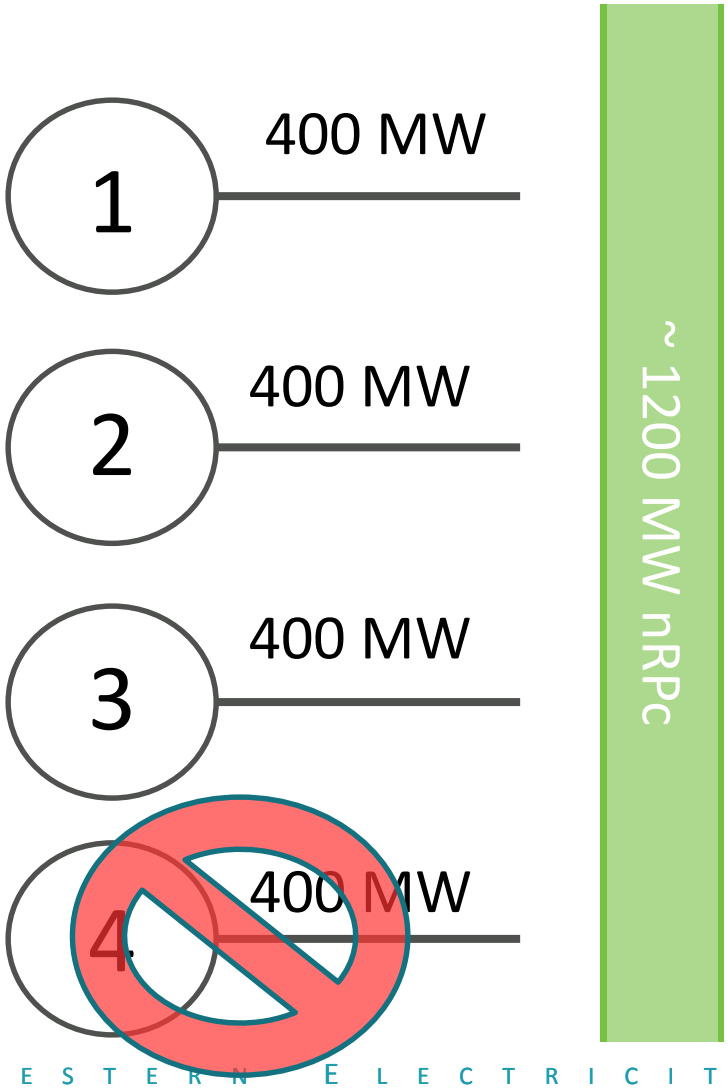
Catterson, Victoria. *132kV Circuit Breaker*. [Photograph]. Retrieved from https://www.flickr.com/photos/cowlet/36524280/

Exercise #1:
BCA associated with 230kV OCB

- Examples of evidence for retention:
  - BCSI protection & reuse/disposal evidence
  - CIP-007-6:
    - Patch Mgmt (R2)
    - Deployed methods to deter, detect, or prevent malicious code (R3)
  - Recovery Plans
  - Developed baseline configurations

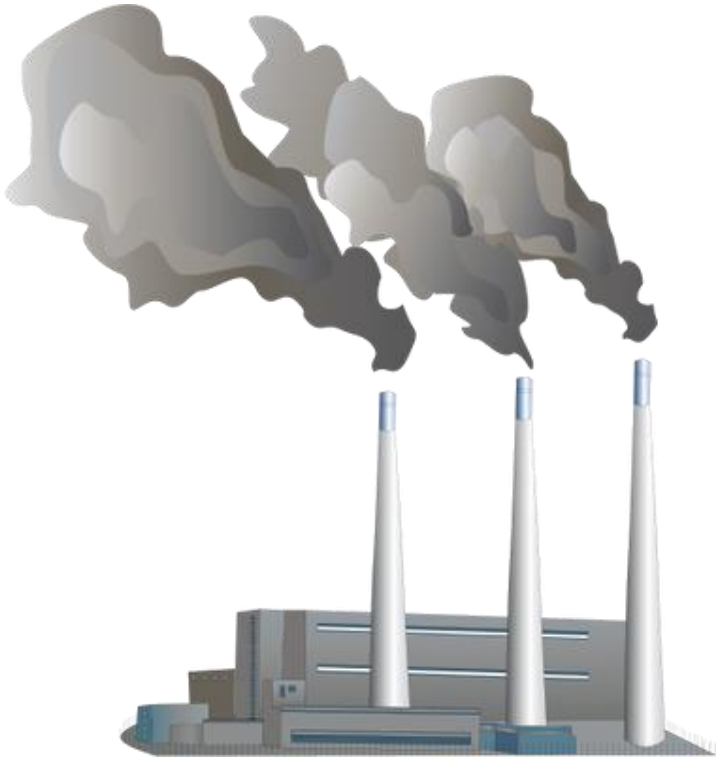
***This review is not intended to be an exhaustive list of what the audit team would evaluate for compliance with decommissioned Cyber Assets.*

Exercise #2:
Medium Impact BES Cyber System



- Scenario:
  - Four 400-MW units
  - Decommission #4
  - Medium → Low Impact
- Retain evidence for this BCS?
  - Retain evidence of:
    - Compliance during audit period
    - Decommissioning activities

Exercise #2:
Medium Impact BES Cyber System



***This is not intended to be an exhaustive list of what the audit team would evaluate for compliance with decommissioned BCS.*

- Examples of evidence for retention:
  - Updated CIP-002 R1 Lists
  - CIP-004-6:
    - Training, PRA, Access & Revocation records
  - ESP & PSP diagrams
  - Recovery Plans for BCS
  - Developed baseline configurations

Exercise #3:
Replacing Workstations

- Scenario:
  - Replacing XP
- Examples of evidence for retention:
  - ESP diagram
  - Backup process
  - Baseline configurations
  - Records of authorized changes
  - Records of how BCSI data destroyed

Windows 10

***This is not intended to be an exhaustive list of what the audit team would evaluate for compliance with decommissioned Cyber Assets.*

Exercise #3:
Replacing Workstations

- New workstations:
  - Vulnerability assessment
  - Developed baseline configuration(s)
  - Updated ESP Diagram(s)
  - CIP-007-6:
    - Physical port protections (R1)
    - Patch Mgmt (R2)
    - System Access (R5)

Windows 10

***This is not intended to be an exhaustive list of what the audit team would evaluate for compliance with new Cyber Assets.*

CIP-011-2 R2 Review

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	Examples of acceptable evidence include, but are not limited to: • Records tracking sanitization actions taken to prevent unauthorized retrieval of BES Cyber System Information such as clearing, purging, or destroying; or • Records tracking actions such as encrypting, retaining in the Physical Security Perimeter or other methods used to prevent unauthorized retrieval of BES Cyber System Information.

- Prevent the unauthorized retrieval of BCSI from Cyber Assets with data storage media
- Records of tracking actions

CIP-011-2 R2 Review

CIP-011-2 Table R2 – BES Cyber Asset Reuse and Disposal			
Part	**Applicable Systems**	**Requirements**	**Measures**
2.2	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Examples of acceptable evidence include, but are not limited to: • Records that indicate that data storage media was destroyed prior to the disposal of an applicable Cyber Asset; or • Records of actions taken to prevent unauthorized retrieval of BES Cyber System Information prior to the disposal of an applicable Cyber Asset.

- Records of Sanitization:
  - Clearing, purging, destroying
  - Erase, destroy, degauss
  - NIST SP 800-88 Revision 1

Expectations at Audit

- Include decommissioned/disposed assets in response to *Notice of Audit – Pre-Audit Data Request* (RFI/CIP Data Set)
- Devices may be included in sample set DR
  - Evidence may not be possible for each sampled requirement but expect to see compliance with sample set questions where applicable
- Audit team may submit DRs or follow up in interviews for additional information on decommissioned assets

Conclusion

- Retain evidence of decommissioned assets applicable to all enforced CIP Standards! (Section C of each standard)
  - Remember to include decommissioned assets in response to *WECC's Notice of Audit – Pre-Audit Data Request* (RFI/CIP Data Set)
  - These devices could be included in the sample set or inquired about during various interviews
- If assets are disposed of or redeployed, be certain to address CIP-011-2 R2 to prevent unauthorized retrieval of BCSI
- If you have questions about evidence of disposed assets or audit expectations, please contact cip@wecc.biz

Contact Information

Holly Eddy
(385)228-2442
heddy@wecc.biz

Eric Weston
(801)819-7630
eweston@wecc.biz