Agenda

• Purpose of CIP-003 R5
• Implementing CIP-003 R5
• Evidence and violations we have seen
• Related CIP standards
What is CIP-003 R5, and why is it important?

- **Purpose:** “Document and implement a program for managing access to protected Critical Cyber Asset information (CCAI).”
- Some CCAI is extremely sensitive and could be used to compromise systems and adversely impact reliability.
R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.

R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

– R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.

– R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.

R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity’s needs and appropriate personnel roles and responsibilities.

R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.
Example Risk:
Contractor goes to another job but still has access.
Where is your CCAI now?
Example Risk:
Employee transferred from IT to Public Relations
Does employee still need access to confidential files?
CIP-003 R4 - Cornerstone to CIP-003 R5

1. Implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.

I. Identify WHO should determine your company’s appropriate protection of CCAI

II. Develop CCAI classification structure

III. HOW to identify and apply appropriate level of protection to all CCAI

IV. Develop process to assess adherence to the CCAI protection process

V. Implement and document the program.

Reference: Standard Review - CIP-003-3 - R4: Information Protection
CIP-003 R5: Controlling Access to CCAI

1. Develop list of personnel responsible for authorizing logical and/or physical access to CCAI
   - Identify name, title, and information for which they are responsible for authorizing access

2. Process to grant access to CCAI

3. Process to annually review access privileges

4. Procedure to annually review the processes for controlling CCAI access

5. Document and implement the program
IDENTIFY ACCESS APPROVERS
R5.1: Develop Authorizer List

• Create list of authorizers and CCAI for which they are responsible
  – May be owners of the information
  – Responsibilities can overlap
  – List should clearly identify information to which the authorizers can approve access

• Best Practice*: Information Rights Management Solution
  – Assign types of access permissions
    ▪ Such as the ability to read-only, update, save, send, print
  – Authenticates access

* Not required
R5.1: Develop Authorizer List

- Best practices* to ensure there are no gaps:
  - Map documents/document types to authorizers
    - Combines R4 and R5 into cohesive program
  - Meet with authorizers and train on expectations
  - Authorizers should be involved in CIP-007 R5.1.3 annual review of user accounts to verify access privileges

* Not required
For R5.1, R5.1.1, and R5.1.2, provide auditors with:

- List of personnel responsible for authorizing logical and/or physical access to CCAI
  - Include authorization rights and responsibilities

- Evidence the list has been verified annually. We’ve seen:
  - Previous list version
  - Revision history
Real-life violations of R5.1, R5.1.1, R5.1.2

• The Responsible Entity maintained a list of designated personnel for authorizing only logical access to CCAI.
• The Responsible Entity did not maintain a list of designated personnel who are responsible for authorizing access to CCAI.
• The Responsible Entity did not identify the personnel by name, title, or the information for which they are responsible for authorizing access.
• The Responsible Entity did not verify at least annually the list of personnel responsible for authorizing access to protected information.
REVIEW OF CCAI ACCESS PRIVILEGES
R5.2: Review CCAI access privileges

1. Identify CCAI access privileges
2. Determine process to grant privileges
   - Do not grant access solely on title, grade level, position
   - Do grant access based on need-to-know
3. Determine process to revoke access
   - Remember temporary leaves and staff transfers
4. Meet with CCAI authorizers and owners
5. Grant access
R5.2: Review CCAI access privileges, con’t.

6. Develop process to review ALL access privileges annually
   — Review all CCAI access privileges
   — Consistent with process to grant and revoke access
   — Confirm access privileges are correct
   — Could be reviewed quarterly with CIP-004 R4

7. Self-Report any discovered gaps

8. Document processes

9. Train authorizers on expectations
For R5.2, provide auditors with...

• Overview of how CCAI access is granted. Include criteria:
  – Based on needs
  – Assigned to appropriate roles/responsibilities

• Evidence demonstrating you followed your process. We’ve seen:
  – Screenshot/log of electronic approval
  – Emails
For R5.2, provide auditors with...

- Overview of process to verify that granted access corresponds with your CCAI access management program. We’ve seen:
  - Documented program
  - RSAW/Narratives
For R5.2, provide auditors with...

• Evidence you verified ALL access privileges, corresponding with your CCAI access management program for the audit period
  - Are access rights or restrictions still appropriate for a given document/document type?
  - Does staff with access still need that access?

• We’ve seen:
  - Access list revision history
  - Emails determining access needs
Real-life violations of R5.2

• The Responsible Entity did not review the access privileges annually.

• The entity did not verify that access privileges correspond with the Responsible Entity’s needs and are assigned to appropriate personnel roles and responsibilities.
PROCESS TO CONTROL CCAI ACCESS
R5.3: Review procedure for controlling access

- Create and document a procedure to annually review processes for controlling CCAI access
- Provide auditors with:
  - Understanding of procedure to annually review the processes for controlling CCAI access
  - Evidence you followed this procedure. We’ve seen:
    - Meeting minutes
    - Previous versions and revision history of program document
Real-life violations of R5.3

• The entity failed to provide evidence that it assessed the processes for controlling access privileges to protected information annually.

• The entity did not provide evidence that it assessed the processes for controlling access to logical privileges to protected information annually.
How does CIP-003 R5 relate to other standards?

- CIP-003 R4 (Information Protection)
- CIP-004 R2.2.3 (Training)
- CIP-004 R4 (Access)
- CIP-006 R1.5 (Review of access authorization)
- CIP-007 R5.1.3 (Review of access privileges)
Gotchas

• Does the process/program for managing CCAI access have to be signed by the Senior Manager?
• If an entity has a violation with its Information Protection program (CIP-003 R4), will it have a violation of its process to grant CCAI access?
Your Access Control Program

- Establishes criteria for managing access to CCAI
- Establishes accountability
  - Identifies ownership/authorizer of CCAI
- Mandates:
  - Review access to CCAI
  - Assess and document the program that controls CCAI
SPP RE Training Videos:
vimeopro.com/sppre/basics

- Audits: Top 10 Ways to Prepare
- CIP Audit: What to Expect
- CIP-005: Electronic Security Perimeter
- CIP-005-3 R3
- CIP-006: Physical Security
- CIP-007 Compliance
- CIP-007: R1 System Configuration
- CIP-007 R3 and R4
- Compliance Education at My Company
- Internal Compliance Programs Q&A
- Event Analysis-Entity Perspective

- Evidence Submission
- Firewalls: 13 Ways to Break Through
- Hashing: How To
- Human Performance - Entity Perspective
- Human Performance - NERC
- Mitigation Plans: Milestones, Completion, and Evidence
- Mock 693 Audit
- Self-Reporting: When and How
- TFE Expectations and Issues
- Training Employees on Compliance