Disclaimer

This NPCC TFIST workshop provides a forum for the presentation and discussion of member experience in the implementation of compliance programs for the NERC CIP Cyber Security Standards. Materials presented or discussed are the presenters’ own interpretation and recommendations and do not necessarily represent those of their organizations or NPCC.
CIP-004 Purpose

Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCA), including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.
CIP-004 Standard Requirements

R1. Awareness
R2. Training
R3. Personnel Risk Assessment
R4. Access
The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive ongoing reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:
The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:

- Direct communications
- Indirect communications
- Management support and reinforcement
CIP-004 R2 – Training

The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to CCA, and review the program annually and update as necessary.
This program will ensure that all personnel having such access to CCA, including contractors and service vendors, are trained within ninety calendar days of such authorization.
Training shall cover policies, access controls, and procedures, and include, at a minimum:

- The proper use of CCA
- Physical and electronic access controls to CCA’s
- The proper handling of CCA Information
- Procedures to recover or re-establish CCA’s
CIP-004 R2 – Training (Cont.)

The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.
The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. Such assessments shall be conducted within thirty days of personnel being granted such access.
The program shall at a minimum:

- Include identity verification (e.g., Social Security Number verification in the U.S.) and seven year criminal check
- Update each personnel risk assessment at least every seven, or for cause
- Document the results of personnel risk assessments
CIP-004 R4 – Access

The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to CCA, including their specific electronic and physical access rights to CCA.
Review list(s) of its personnel who have such access to CCA’s quarterly

- Update the list(s) within seven calendar days of any change of personnel with such access, or any change in access rights of such personnel.

- The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
The Responsible Entity shall revoke access to CCA’s:

- Within 24 hours for personnel terminated for cause
- Within seven calendar days for personnel who otherwise no longer require such access