Standard CIP-009-1

-- Cyber Security --
Recovery Plans for
Critical Cyber Assets
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-009 Purpose

Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.
R1 – Recovery Plans – The responsible entity shall create and annually review recovery plans for Critical Cyber Assets.

- Specify the required actions in response to events or conditions of varying duration and severity that would activate the Recovery Plan.
- Define the roles and responsibilities of responders
Standard Requirements

- R2 – Exercises – The Recovery Plans shall be exercised at least annually.
  - Paper Drills
  - Full Operational Exercise
  - Actual Incident
Panel Discussion
Standard Requirements

- R3 – Change Control – Recovery
  Plans shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident.
Panel Discussion
Standard Requirements

- R4 – Back-up and Restore – The Recovery Plan shall include processes and procedures for the back-up and storage of information required to successfully restore Critical Cyber Assets.
Panel Discussion
R5 – Testing Back-up Media – Information essential to recovery, that is stored on backup media, shall be tested at least annually to ensure that the information is available. Testing can be completed off site.
Panel Discussion