CIP-009-5: Recovery Plans for BES Cyber Systems

NPCC Workshop
March 24-25, 2015

Frank Lembo
NPCC Auditor
R1.4: One or more processes to verify the successful completion of the backup processes in Part 1.3 and to address any backup failures.

- An example of evidence may include, but is not limited to, logs, workflow or other documentation confirming that the backup process completed successfully and backup failures, if any, were addressed.
CIP-009-5: Recovery Plans for BES Cyber Systems

V5 Additions

R1.5: One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery.

- An example of evidence may include, but is not limited to, procedures to preserve data, such as preserving a corrupted drive or making a data mirror of the system before proceeding with recovery.
CIP-009-5: Recovery Plans for BES Cyber Systems

V5 Additions

R2.3: Test each of the recovery plans referenced in Requirement R1 at least once every 36 calendar months through an operational exercise of the recovery plans in an environment representative of the production environment.

- Examples of evidence may include, but are not limited to, dated documentation of:
  - An operational exercise at least once every 36 calendar months between exercises, that demonstrates recovery in a representative environment; or
  - An actual recovery response that occurred within the 36 calendar month timeframe that exercised the recovery plans.
CIP-009-5 FAQ: Recovery Plan Testing

R2: What level of testing is expected for the Recovery Plans?

> A recovery plan test that incorporates all of the criteria of the entity’s recovery plan document, based on the scenario of the test, including evidence of recovery, personnel communications, plan activation thresholds, documented recovery procedures, lessons learned, etc. is what’s required.

Be it an actual incident, paper drill, or operational exercise, the criteria of the Standard and the entity’s recovery procedures need to be documented as proof of compliance for recovery plan testing.