Lessons Learned from Commission-Led CIP Reliability Audits: Federal Energy Regulatory Commission Staff Report

Walter Wright, Jr.
wwright@mwlaw.com
(501) 688.8839

10/14/2021

The Federal Energy Regulatory Commission ("FERC") staff prepared an October 8th report titled:

Lessons Learned from Commission-Led CIP Reliability Audits ("Report")

The *Report* is intended to offer recommendations to assist users, owners and operators of bulk-power systems to improve their compliance with the Critical Infrastructure Protection ("CIP") Reliability Standards and their overall cyber security posture.

Electric utilities that own, operate or use the bulk electric system must comply with the CIP standards. Compliance with such standards can obviously be expensive. Failure to meet these standards can result in noncompliance penalties. Difficulties associated with compliance can increase as technology and cyber security concerns evolve.

Section 215 of the Federal Power Act requires an FERC-certified Electric Reliability Organization to develop mandatory and enforceable Reliability Standards. Such Standards are subject to FERC review and approval. They are designed to mitigate the cyber security and fiscal security risks to the relevant facilities which, if destroyed, degraded, or otherwise rendered unavailable as a result of a security interest, would affect the reliable operation of the Bulk-Power System.

The *Report* states that the FERC staff completed non-public CIP audits of several bulk electric system registered entities during fiscal year 2021. The audits are stated to have evaluated registered entities' compliance with CIP Reliability Standards.

FERC staff are stated to have determined that:

. . . While most of the cyber security protection processes and procedures adopted by the registered entities met the mandatory requirements of the CIP Reliability Standards, there were also potential compliance infractions.

Further, staff is also stated to have identified practices not required by the CIP Reliability Standards that could improve security.

The *Report's* recommendations include:

- Enhance policies and procedures to include evaluation of Cyber Asset misuse and degradation during asset categorization;
- Properly document and implement policies, procedures and controls for low-impact transient cyber assets;

- Enhance recovery and testing plans to include a sample of any offsite backup images in the representative sample of data used to test the restoration of bulk-electric system cyber systems;
- Improve vulnerability assessments to include credential-based scans of cyber assets; and
- Enhance internal compliance and controls programs to include control documentation processes and associated procedures pertaining to compliance with the CIP Reliability Standards.

A copy of the *Report* can be downloaded here.