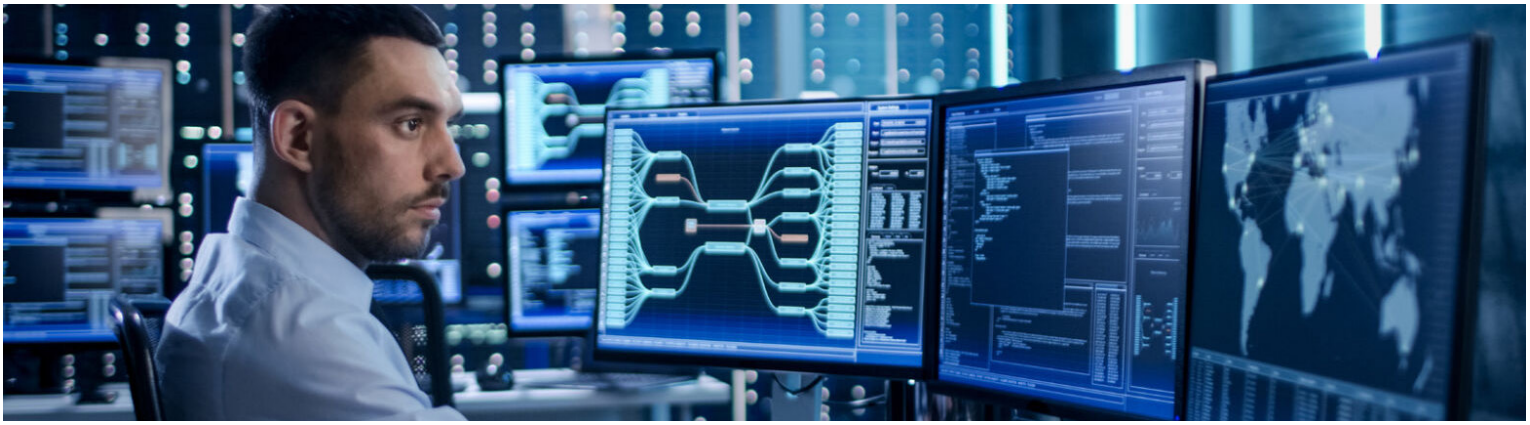
CIP-014-3 (Physical Security) – Post Assessment Support



NERC Compliance Solutions and Best Practices

This proposition focuses on enhancing shareholder value and corporate compliance reputation by mitigating the risk of non-recoverable NERC fines, improving audit readiness, eliminating silos, enhancing operational efficiency, streamlining workflows and establishing a centralized document repository for core compliance data.

Your utility's NERC CIP compliance responsibilities and evidentiary needs can arise from multiple interconnected regulatory obligations, of which NERC CIP-014 is only one. Periodic NERC CIP compliance reviews and BES upgrades can trigger compliance obligations for your company with NERC CIP standards, other than CIP-014. This knowledge is important to help keep your company in compliance.

There are four NERC CIP compliance standards that are directly influenced by the results of your CIP-014 assessment: CIP-002, CIP-005, CIP-006, and CIP-011. Due to the breadth of its CIP related advisory services, TRC is optimally positioned to follow through with additional NERC compliance advisory support to our clients.

For example, CIP-002 (Cyber Security — BES Cyber System Categorization), it is observed that the CIP-014 Applicability table (in Section 4.1.1.2) is identical to the CIP-002 NERC CIP Medium Impact Criteria table (in Attachment 1, Section 2.5). TRC is in position to ensure explicit communication with your CIP-002 SMEs to update the NERC CIP Medium Impact and NERC CIP Low Impact lists. Furthermore, TRC can provide the corresponding documentation based on the release (Version 8) of NERC's Evidence Request Tool (ERT) formatted spreadsheet.

While TRC is actively performing its Physical Security evaluations in your substations or control centers (both operating and security control centers), the Electronic Security Perimeters (ESP) and Physical Security Perimeters (PSP) are readily available to be formally documented and certified. TRC offers these ancillary NERC compliance support services for most of your CIP-005 and CIP-006 standard requirement obligations.

Lastly, TRC experts are experienced with handling protected cyber assets, removable media, and other sensitive equipment that may contain BES cyber security information (BCSI) related to CIP-011. As the CIP-014 engagement is being closed out, TRC is in position to ensure all cyber system assets were properly disposed of or retained for reuse.