Office of NERC Compliance

CASE STUDY: CRITICAL CYBER SECURITY ASSET IDENTIFICATION

CRITICAL ASSET CHALLENGE

A top-five generation utility needed to determine if any of its assets were critical cyber security assets, per the North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. Due to a lack of NERC expertise, time, and resources, it reached out to Certrec, through its Office of NERC Compliance, to assist in quantifying and qualifying its critical assets across a number of its Generation plants.

CERTREC APPROACH

Employing its deep regulatory and compliance expertise, Certrec recommended developing a Risk-Based Assessment Methodology and performing engineering assessments meeting the NERC CIP Standards and Requirements that included:

- Control centers and backup control centers
- Transmission substations
- Generation resources
- Systems and facilities critical to system restoration,
- Systems and facilities critical to automatic load shedding
- Special Protection Systems

ASSESSMENT ACTIONS

To produce the insight the utility sought from the Risk-Based Assessment, Certrec's NERC compliance experts assessed the following:

- Determine if the plants meet the critical asset criteria by assessing impact on the facility, on the reliability of the associated transmission system and on the bulk electric system using industry standard methods
- Develop risk-based assessment methodology per CIP-002-3 R1 for each facility
- Perform Engineering assessments based upon the assessment methodology and develop a list of identified Critical Assets per CIP-002-3 R1, including transmission sub-stations
- Provide a final report summarizing the activities performed and results / conclusions

CERTREC

Helping You Manage the Regulatory Process to Your Advantage

4200 S. Hulen St., Fort Worth, TX 76109
817.738.7661 / www.certrec.com