

NEW YORK STATE RELIABILITY COUNCIL
MEETING 234: October 12, 2018
NPCC Board of Directors Report

The NPCC Board of Directors (BOD) meeting was held on September 6th. The following is a summary of the NPCC President's Report to the BOD.

15 Year Reflections – August 14, 2003

On August 14, 2003, large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power blackout. The outage affected an area with an estimated 50 million people and 61,800 megawatts (MW) of electric load in the states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey and the Canadian province of Ontario. The blackout began a few minutes after 4:00 pm Eastern Daylight Time, and power was not restored for two days in some parts of the United States. Parts of Ontario suffered rolling blackouts for more than a week before full power was restored. Factors leading up to the collapse included: lack of situational awareness due to the unavailability of state estimators and contingency analysis; excessive tree growth on the rights-of-way; and insufficient operational planning studies; or more colloquially – tools, trees and training.

In direct response to the blackout, the Energy Policy Act was enacted in 2005 in the U.S. that established an ERO and provided for the delegation of authorities to Regional Entities. Reliability standards for operations and planning become mandatory, including requirements around Energy Management Systems (EMS), situation awareness and vegetation management, and standards for the cyber and physical protection of critical infrastructure were created. Compliance monitoring and enforcement activities, including the imposition of financial penalties, were initiated and detailed events analysis reporting and investigations were conducted.

Reflecting on the significant enhancements made to the reliability construct since the August 2003 blackout, much has been done, but considering the emerging risks facing a changing industry that were identified in NERC's 2018 State of Reliability Report, much remains to be addressed.

Supply Chain Update

On August 10, 2017, the NERC Board of Trustees approved the proposed Supply Chain Risk Management requirements: Cyber Security – Supply Chain Risk Management – CIP-005-6, CIP-010-3, and CIP-013-1. As part of the approval, the Board directed NERC management to study the nature and complexity of cyber security supply chain risks, including risks associated with low impact assets not currently subject to the Supply Chain Standards. NERC staff provided an interim report to the BOT during its August 2018 meeting that included a summary of the Supply Chain Risk Assessment Report that was prepared for NERC by the Electric Power Research Institute (EPRI). Key takeaways from that report include: the identification of some ten emerging practices that could reduce additional supply chain risk, the recommendation for additional research to model and assess the impact of a common-mode threat, as well as suggested data analysis techniques for assessing vulnerabilities.

In addition to the staff presentation, the North American Transmission Forum referenced a Cyber Security Supply Chain Risk Management Guidance document that it had made available as a part of its policy input to the MRC and the BOT's August meetings.