Federal Energy Regulatory Commission
December 21, 2017
Open Commission Meeting
Staff Presentation
Item E-1

“Good Morning, Mr. Chairman and Commissioners.

“Item E-1 is a draft Notice of Proposed Rulemaking (NOPR) that proposes, pursuant to section 215(d)(5) of the Federal Power Act, directing the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the NERC Critical Infrastructure Protection (CIP) Reliability Standards to improve the mandatory reporting of Cyber Security Incidents. The draft NOPR is based on a concern that the current reporting threshold for Cyber Security Incidents in the CIP Reliability Standards may understate the true scope of cyber-related threats facing the bulk electric system. As noted in the draft NOPR, the lack of any reported Cyber Security Incidents in either 2015 or 2016 suggests a gap in the current mandatory reporting requirements.

“This gap was highlighted in NERC’s 2017 State of Reliability Report, which noted that “[w]hile there were no reportable cyber security incidents during 2016 and therefore none that caused a loss of load, this does not necessarily suggest that the risk of a cyber security incident is low.” The draft NOPR notes that the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to fifty-nine cybersecurity incidents within the Energy Sector, which includes the electric subsector, in 2016.

“In order to address this gap and provide more timely awareness of cyber threats facing the bulk electric system, the draft NOPR proposes to direct NERC to develop modifications to the CIP Reliability Standards to include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS). In addition, the draft NOPR proposes to direct NERC to modify the CIP Reliability Standards to specify the required information in Cyber Security Incident reports to improve the quality of reporting and allow for ease of comparison and analysis by ensuring that each report includes certain key information regarding the incident. The draft NOPR also proposes to direct NERC to modify the CIP Reliability Standards to establish a deadline for filing a report with the Electricity Information Sharing and Analysis Center (E-ISAC) and ICS-CERT once a compromise or disruption to reliable bulk electric system operation, or an attempted compromise or disruption, is identified by a responsible entity. Finally, the draft NOPR proposes to direct NERC to file annually an anonymized report providing an aggregated summary of the reported information with the Commission.

“As discussed in the draft NOPR, the proposed modifications will enhance awareness for NERC, industry, the Commission, other federal and state entities, and interested stakeholders regarding existing and developing cyber security threats.

“This concludes the presentation. I will be happy to take any questions you may have.”