Federal Energy Regulatory Commission expands cybersecurity incident reporting requirements

Michael W. Wise, Colin M. Battersby, Hussein Jaward, CIPP/US | Friday, June 28, 2019

Last week, the Federal Energy Regulatory Commission adopted a North American Electric Reliability Corporation-proposed Reliability Standard that imposes new cybersecurity incident reporting requirements upon responsible entities, including balancing authorities, distribution providers, generator operators, generator owners, reliability coordinators, transmission operators, and transmission owners.

Whereas previously, responsible entities were only required to report cybersecurity incidents that have "compromised or disrupted one or more reliability tasks," the new Reliability Standard requires responsible entities to also report incidents that "compromise, or attempt to compromise" certain systems. Actual compromises or disruptions of reliability tasks, electronic security perimeters or electronic access or control monitoring systems are to be reported within one hour of discovery. Meanwhile, attempts to compromise electronic security perimeters, electronic access or control monitoring systems, or physical security perimeters are to be reported by the end of the first calendar day after discovery. Importantly, the new Reliability Standard gives responsible entities some autonomy in developing criteria to define what constitutes an attempt to compromise the applicable systems.

Additionally, the reports, which are to be made to the Electricity Information Sharing and Analysis Center and the United States Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team, must document the subject incident's functional impact, attack vector, and the achieved or attempted level of intrusion.

Failure to comply with these requirements carries substantial civil penalties.

The new regulation is in keeping with growing industry and regulatory awareness of cyber threats facing the nation's electrical grid. Just a few weeks ago, for example, Texas enacted two new laws attempting to address its own electric power industry's cybersecurity vulnerabilities. The electric power industry should remain vigilant for forthcoming state and federal laws and regulations aimed at addressing cyber threats.

Attorneys from McDonald Hopkins' Data Privacy and Cybersecurity Practice Group and Energy Practice Group are available to guide members of the electric power industry through these challenging laws and regulations.

Federal Energy Regulatory Commission expands cybersecurity incident reporting requirements

Michael W. Wise

Colin M. Battersby

Hussein Jaward, CIPP/US