July 27, 2018

FERC Expands Cyber Security Incident Reporting Requirements

Recognizing the growing cyber threats facing the country's bulk electric system, the Federal Energy Regulatory Commission (the Commission) recently issued a rule that will increase the reporting requirements for those entities with assets that make up the nation's bulk electric system. In Order No. 848,[1] issued on July 19, the Commission directs the North American Electric Reliability Corp. (NERC) to develop modifications to its Reliability Standards to expand mandatory reporting of cyber security incidents, including attempts that might facilitate subsequent efforts to harm reliable operation of the electric system.

NERC, the electric reliability organization for North America, has established mandatory Critical Infrastructure Protection (CIP) Reliability Standards designed to secure the cyber assets required for operating North America's bulk power system. Those requirements include Reliability Standard CIP-008-5 (Cyber Security — Incident Reporting and Response Planning),[2] but those reporting requirements currently apply only for cyber incidents that "compromised or disrupted one or more reliability tasks." The Commission concluded that with such limited reporting requirements, the true scope of cyber-related threats facing the North America grid is understated.

There is wide recognition and numerous reports documenting the increasing frequency and complexity of these cyber security threats. For example, the National Cybersecurity and Communications Integration Center (NCCIC) recently outlined ongoing activity by Russian government actors characterized as:

> a multi-stage intrusion campaign by [] cyber actors who targeted small commercial facilities' networks where they staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the Russian government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).[3]

Given its concern with the growing threats to the power grid, the Commission in Order No. 848 directs that NERC implement the following four changes to strengthen the current Cyber Security Incident reporting requirement: (1) each responsible entity must report Cyber Security Incidents that compromise, *or attempt to compromise*, that entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS);[4] (2) information in Cyber Security Incident reports must include certain minimum information designed to improve the quality of reporting and to allow for ease of comparison by ensuring that each report includes specified fields of information; (3) deadlines for filing Cyber Security Incident reports must be established based on when the responsible entity identifies a compromise or disruption to reliable operation of its facilities in the bulk electric system; and (4) Cyber Security Incident reports should continue to be sent to the Electricity Information Sharing and Analysis Center (E-ISAC), rather than the Commission, but the reports should also be sent to the Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). Further, the Commission requires that NERC annually file with the Commission a public, anonymized summary of the reports received over the past year.

Providing more specificity on the content of Cyber Security Incident reports, Order No. 848 directs that the minimum set of attributes to be reported to NERC include (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack vector that was used to achieve or attempted to achieve the Cyber Security Incident; and (3) the level of intrusion that was achieved or attempted.[5] NERC may also augment the list should it determine that additional information would benefit situational awareness of cyber threats.[6]

These modifications that the Commission has directed NERC to make could have significant implications for responsible entities and their existing reporting processes. Registered entities should ensure their familiarity with these modified, mandatory standards and work to ensure adequate cyber awareness, monitoring and reporting capabilities.

Day Pitney's Energy & Utilities and Cybersecurity & Data Protection practices will continue to monitor developments in this area and inform our clients and friends as appropriate. If you have questions, please call any of us.

---

[1] *Cyber Security Incident Reporting Reliability Standards*, Final Rule, 164 FERC ¶ 61,033 (2018) (Order No. 848). Order No. 848 takes effect 60 days after publication in the Federal Register. NERC must submit the directed modifications within six months of that effective date.

[2] The NERC CIP Standards are available here.

[3] *See* United States Computer Emergency Readiness Team, Alert TA18-074A (revised Mar. 16, 2018), available here. NCCIC is currently conducting a series of webinars on Russian government cyber activity against critical infrastructure.

[4] The NERC Glossary defines “ESP” as “[t]he logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol.” The NERC Glossary defines “EACMS” as “Cyber Assets that perform electronic access control or electronic access monitoring of the Electronic Security Perimeter(s) or BES Cyber Systems. This includes Intermediate Systems.”

[5] Order No. 848 at P 88.

[6] These attributes are the same as attributes already used by the Department of Homeland Security (DHS) for its multisector reporting and summarized by DHS in an annual report. *See* 2016 ICS-CERT Year in Review.

Authors



David T. Doot
Of Counsel

Hartford, CT | (860) 275-0102

dtdoot@daypitney.com



Evan C. Reese III
Partner

Washington, D.C. | (202) 218-3917

ereese@daypitney.com



Patrick M. Gerity
Counsel

Hartford, CT | (860) 275-0533

pmgerity@daypitney.com