First Look: FERC Order 848 - Cyber Security Incident Reporting Reliability Standards

Directs NERC to modify its Critical Infrastructure Protection Reliability Standards to broaden and standardize mandatory reporting of cyber security incidents.

Updated last **August 2, 2018**
for the 7/19/2018 Final Rule, published in the Federal Register on 7/31/2018.

WHAT IT DOES

On July 19, 2018, the Federal Energy Regulatory Commission (FERC) issued a Final Rule on Cyber Security Incident Reporting Reliability Standards, 164 FERC ¶ 61,033. The Rule was published in the Federal Register on July 31, 2018, and will become effective on October 1, 2018.

The Rule directs the North American Electric Reliability Corporation (NERC) to develop, within six months of the Rule's effective date, modifications to the Critical Infrastructure Protection Reliability Standards (CIP Standards) that NERC enforces on U.S. utilities and other electric system participants ("responsible entities"). In an effort to ensure tht the power sector is alert to developing and emerging threats, NERC's new standards must direct responsible entities to report not only cyber security incidents that have actually compromised or disrupted their systems, but also *attempted* breaches that might facilitate future attempts to harm the system. FERC is directing NERC to mandate reporting of cybersecurity incidents that either do or attempt to compromise a responsible entity's electronic security perimeter (ESP) or electronic access control or monitoring system (EACMS). NERC must also standardize reporting requirements to ensure that incident reports include certain minimum information, impose reporting timelines, and specify that reports be sent to both the Electricity Information Sharing and Analysis Center within NERC and the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team.

FERC has directed NERC to take incidents' threat level into account as it develops the thresholds at which entities will be required to report incidents, and the timelines within which they must be reported. Entities will need only report incidents meeting a certain threat level, and will be required to report those incidents with the greatest potential or actual adverse impact to the grid more quickly than they do incidents with less impact.

The new NERC standards will supersede the current CIP-008-5 (Cyber Security-Incident Reporting and Response Planning).

PRIMARY AUTHOR

Sarah Rispin Sedlak, J.D.

EDITOR(S)

Sarah Rispin Sedlak, J.D.

ENERGY SUBCATEGORY

Production, Conversion, Distribution

RECOMMENDED CITATION

Duke SciPol, “First Look: FERC Order 848 on Cyber Security Incident Reporting Reliability Standards” available at <http://scipol.duke.edu/content/ferc-order-848-cyber-security-incident-reporting-reliability-standards> (Aug. 2, 2018).

LICENSE