161 FERC ¶ 61,003
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Neil Chatterjee, Chairman;
Cheryl A. LaFleur, and Robert F. Powelson.

Cyber Systems in Control Centers Docket No. RM16-18-000

ORDER TERMINATING PROCEEDING

(Issued October 2, 2017)

1. On July 21, 2016, the Commission issued a Notice of Inquiry (NOI), pursuant to section 215 of the Federal Power Act (FPA),[1] seeking comment on the need for, and possible effects of, modifications to the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) Reliability Standards to address the cybersecurity of control centers used to monitor and control the bulk electric system.[2] We are exercising our discretion to terminate this proceeding.

2. The NOI was prompted in part because of a 2015 cyber attack in Ukraine (Ukraine event) that significantly disrupted Ukraine's electric grid.[3] On December 23, 2015, three regional electric power distribution companies in Ukraine experienced a cyber attack resulting in power outages that affected at least 225,000 customers. On February 25, 2016, the U.S. Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team issued an alert stating that the Ukraine event

[1] 16 U.S.C. 824o. Section 215(a)(3) of the FPA defines "Reliability Standard" to include "…requirements for the operation of existing bulk-power system facilities, including cybersecurity protection…."

[2] *Cyber Systems in Control Centers*, Notice of Inquiry, 156 FERC ¶ 61,051 (2016).

[3] The Electricity Information Sharing and Analysis Center (E-ISAC) and SANS Industrial Control Systems concluded in a joint report that the Ukraine event is the first publicly acknowledged cyber incident to result in power outages. E-ISAC, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, at vi (March 18, 2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

was synchronized and coordinated.[4] The alert reported that the cyber attacks at each company occurred within 30 minutes of each other and affected multiple central and regional facilities.[5]

3. In the NOI, the Commission sought comment on possible modifications to the CIP Reliability Standards, and potential operational impacts thereof, involving the following cyber strategies:

> (1) isolating BES Cyber Systems in control centers performing transmission operator functions from the Internet; and
>
> (2) using computer administration practices that prevent unauthorized programs from running (i.e., "application whitelisting") for cyber systems in control centers.

The questions in the NOI were informed by DHS advisories, alerts, and guidance that discuss using isolation and whitelisting as mitigation strategies for malicious activity and E-ISAC alerts and guidance discussing the use of whitelisting.[6] The Commission

---

[4] DHS, Alert (IR-ALERT-H-16-056-01) *Cyber-Attack Against Ukrainian Critical Infrastructure* (February 25, 2016), https://icscert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[5] *Id.*

[6] *See*, *e.g.*, Notice of Inquiry, 156 FERC ¶ 61,051 at PP 5-6, 10, 12-13; *see also* DHS, *Seven Steps to Effectively Defend Industrial Control Systems*, https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf; DHS, *ICS Focused Malware*, https://ics-cert.us-cert.gov/advisories/ICSA-14-178-01; DHS, *CrashOverride Malware*, https://www.us-cert.gov/ncas/alerts/TA17-163A; DHS, *HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure*, https://www.us-cert.gov/ncas/alerts/TA17-164A; DHS, *Guidelines for Application Whitelisting in Industrial Control Systems*, https://ics-cert.us-cert.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf; DHS, *Targeted Cyber Intrusion Detection and Mitigation Strategies (Update B)*, https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B; E-ISAC, *Modular Malware Targeting Electric Industry Assets in Ukraine*, http://www.nerc.com/pa/rrm/bpsa/Alerts%20DL/NERCAlert_A-2017-06-13-01_Modular-Electric-Industry-Malware.pdf.

received eighteen comments in response to the NOI generally opposing modifications to the CIP Reliability Standards at this time.

4. After reviewing the NOI comments, the Commission determines to exercise its discretion and terminate this proceeding. Currently, the CIP Reliability Standards allow responsible entities flexibility on how to implement various required security controls. With continued information sharing and dissemination of lessons-learned among stakeholders, responsible entities can better implement security controls, including, when appropriate, isolation and whitelisting, achieving the objectives of the CIP Reliability Standards.

5. The record in this proceeding does not support requiring the use of isolation or whitelisting in the CIP Reliability Standards at this time. While isolation and whitelisting can be effective strategies under certain circumstances, these strategies also present certain risks, and careful evaluation of these strategies is needed to mitigate these risks. For example, a delay or mistake in updating a whitelist might prevent operation of a necessary function, and sustained isolation of certain BES Cyber Systems from the Internet could impede an entity's ability to maintain awareness of the conditions on the Bulk-Power System and achieve business efficiencies under normal conditions. In addition, a Reliability Standard requiring isolation or whitelisting may be difficult to develop given the diversity of configurations existing across the Bulk-Power System. Accordingly, we exercise our discretion to terminate this proceeding.

6. While we exercise our discretion to terminate this proceeding, we will continue to support attention to isolation and segmentation, whitelisting, and other cybersecurity strategies. Commission staff will engage with NERC, industry, and other stakeholders to look for opportunities to explore these strategies more thoroughly and encourage their use in appropriate circumstances, seeking ways to achieve their potential benefits while addressing possible risks. As part of that engagement, we encourage Commission staff and NERC to work together to develop, as they deem appropriate, reports, guidance documents, workshops, or other efforts to evaluate these strategies and support the deployment of tools and technologies that improve the cybersecurity of the Bulk-Power System.

The Commission orders:

Docket No. RM16-18-000 is hereby terminated.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

Document Content(s)