156 FERC ¶ 61,051
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Docket No. RM16-18-000

Cyber Systems in Control Centers

(Issued July 21, 2016)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of Inquiry.

SUMMARY: In this Notice of Inquiry, the Federal Energy Regulatory Commission seeks comment on possible modifications to the Critical Infrastructure Protection Reliability Standards regarding the cybersecurity of Control Centers used to monitor and control the bulk electric system in real time.

DATES: Comments are due **[INSERT DATE 60 days after publication in the FEDERAL REGISTER]**.

ADDRESSES: You may submit comments, identified by docket number and in accordance with the requirements posted on the Commission's website, http://www.ferc.gov. Comments may be submitted by any of the following methods:

- Agency Website: Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format, at http://www.ferc.gov/docs-filing/efiling.asp.

- Mail/Hand Delivery: Those unable to file electronically must mail or hand deliver comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426.

Instructions: For detailed instructions on submitting comments and additional information on the rulemaking process, see the Comment Procedures Section of this document.

FOR FURTHER INFORMATION CONTACT:

David DeFalaise (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8180
David.DeFalaise@ferc.gov

Robert T. Stroh (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-8473
Robert.Stroh@ferc.gov

SUPPLEMENTARY INFORMATION:

156 FERC ¶ 61,051
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF INQUIRY

(Issued July 21, 2016)

1. In this Notice of Inquiry, pursuant to section 215 of the Federal Power Act (FPA),[1] the Commission seeks comment on the need for, and possible effects of, modifications to the Critical Infrastructure Protection (CIP) Reliability Standards regarding the cybersecurity of Control Centers used to monitor and control the bulk electric system in real time.[2] Cyber systems are used extensively for the operation and maintenance of interconnected transmission networks.[3] A 2015 cyberattack on the electric grid in

[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] NERC defines "Control Center" as "[o]ne or more facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in realtime to perform the reliability tasks, including their associated data centers…." NERC Glossary of Terms Used in Reliability Standards (May 17, 2016) at 33 (NERC Glossary).

[3] Cyber systems are referred to as "BES Cyber Systems" in the CIP Reliability Standards. The NERC Glossary defines BES Cyber Systems as "One or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC Glossary at 15. The NERC Glossary defines "BES Cyber Asset" as "A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed,

(continued…)

Ukraine is an example of how cyber systems used to operate and maintain interconnected networks, unless adequately protected, may be vulnerable to cyberattack. While certain controls in the CIP Reliability Standards may reduce the risk of such attacks,[4] the Commission seeks comment on whether additional controls should be required.

2. Specifically, as discussed below, the Commission seeks comment on possible modifications to the CIP Reliability Standards - and any potential impacts on the operation of the Bulk-Power System resulting from such modifications - to address the following matters: (1) separation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions; and (2) computer administration practices that prevent unauthorized programs from running, referred to as "application whitelisting," for cyber systems in Control Centers.

---

degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the Bulk Electric System. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact. Each BES Cyber Asset is included in one or more BES Cyber Systems." *Id.*

[4] *See, e.g.*, Reliability Standard CIP-005-5 (Electronic Security Perimeter(s)), Requirement R2, which protects against unauthorized interactive remote access; Reliability Standard CIP-006-6 (Physical Security of BES Cyber Systems), Requirement R2, which protects against unauthorized physical access and Reliability Standard CIP-007-6 (System Security Management), Requirement R3, which protects against malware.

I. Background

3. On January 28, 2008, the Commission approved an initial set of eight CIP Reliability Standards pertaining to cybersecurity.[5] In addition, the Commission directed NERC to develop certain modifications to the CIP Reliability Standards. Since 2008, the CIP Reliability Standards have undergone multiple revisions to address Commission directives and respond to emerging cybersecurity issues.

4. On December 23, 2015, three regional electric power distribution companies in Ukraine experienced a cyberattack resulting in power outages that affected at least 225,000 customers. An analysis conducted by a team from the Electricity Information Sharing and Analysis Center (E-ISAC) and SANS Industrial Control Systems (SANS ICS) observed that "the cyber attacks in Ukraine are the first publicly acknowledged incidents to result in power outages."[6]

5. On February 25, 2016, the U.S. Department of Homeland Security (DHS) Industrial Control Systems Cyber Emergency Response Team issued an "Alert" in

[5] *Mandatory Reliability Standards for Critical Infrastructure Protection*, Order No. 706, 122 FERC ¶ 61,040, *denying reh'g and granting clarification*, Order No. 706-A, 123 FERC ¶ 61,174 (2008), *order on clarification*, Order No. 706-B, 126 FERC ¶ 61,229 (2009), *order denying clarification*, Order No. 706-C, 127 FERC ¶ 61,273 (2009).

[6] E-ISAC, Analysis of the Cyber Attack on the Ukrainian Power Grid (March 18, 2016) at 3, http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

response to the Ukraine incident.[7] The Alert stated that the cyberattack was sophisticated and well planned. The Alert reported that the cyberattacks at each company occurred within 30 minutes of each other and affected multiple central and regional facilities. The Alert also explained that during the cyberattacks:

> malicious remote operation of the breakers was conducted by multiple external humans using either existing remote administration tools at the operating system level or remote industrial control system (ICS) client software via virtual private network (VPN) connections. The companies believe that the actors acquired legitimate credentials prior to the cyber-attack to facilitate remote access.

In addition, the Alert reported that the affected companies indicated that the attackers wiped some systems at the conclusion of the cyberattack, which erased selected files, rendering systems inoperable.

6. In response to the Ukraine incident, the Alert recommended the following key examples of best practice mitigation strategies:

> procurement and licensing of trusted hardware and software systems; knowing who and what is on your network through hardware and software asset management automation; on time patching of systems; and strategic technology refresh.[8]

---

[7] *See* Department of Homeland Security, Alert (IR-ALERT-H-16-056-01) *Cyber-Attack Against Ukrainian Critical Infrastructure* (February 25, 2016) (Alert), https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

[8] *Id.* at Mitigation Section. By "strategic technology refresh," the Alert referred to the benefit of replacing legacy cyber systems that no longer receive security patches and, as a result, might not be secure.

II. Request for Comments

7. The Commission seeks comment on whether to modify the CIP Reliability Standards to better secure Control Centers from cyberattacks. The Commission also seeks comment on the potential consequences or complications arising from implementing such modifications. In response to lessons learned from the Alert and analyses of the Ukraine incident, the Commission seeks comment on whether to modify the CIP Reliability Standards to require: (1) separation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions; and (2) "application whitelisting" for BES Cyber Systems in Control Centers.

A. Isolation of Transmission Operator Control Centers from the Internet

8. In response to the Ukraine incident, the Alert recommended that:

> [o]rganizations should isolate [industrial control system] networks from any untrusted networks, especially the Internet. All unused ports should be locked down and all unused services turned off. If a defined business requirement or control function exists, only allow real-time connectivity to external networks. If one-way communication can accomplish a task, use optical separation ('data diode'). If bidirectional communication is necessary, then use a single open port over a restricted network path.

9. Commission-approved Reliability Standard CIP-007-6, Requirement R1 (Ports and Services), Part 1.1 requires, where technically feasible, unused logical ports to be disabled.[9] In addition, Reliability Standard CIP-007-6, Requirement R1, Part 1.2 requires

[9] Logical ports are connection points where two applications communicate to identify different applications or processes running on a cyber asset.

protection of physical ports against unnecessary use.[10] These requirements therefore address the Alert's recommendation that "[a]ll unused ports should be locked down and all unused services turned off."

10. The current CIP Reliability Standards do not require isolation between the Internet and BES Cyber Systems in Control Centers performing transmission operator functions through use of physical (hardware) or logical (software) means. Although BES Cyber Systems are protected by electronic security perimeters and the disabling of unused logical ports, BES Cyber Systems are permitted, within the scope of the current CIP Reliability Standards, to route, or connect, to the Internet.[11] Requiring physical separation between the Internet and cyber systems in Control Centers performing transmission operator functions would require data connections to Control Centers or other facilities owned by transmission operators over dedicated data lines owned or leased by the transmission operator, rather than allowing communications over the Internet.[12] Logical separation, in some contexts, can achieve a similar objective through different means.

---

[10] A physical port serves as an interface or connection between a cyber asset and another cyber asset, or peripheral device, using a physical medium such as a cable.

[11] NERC defines an electronic security perimeter as "the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." NERC Glossary at 39.

[12] *See* Alert at Mitigation Section; *see also* Department of Homeland Security, *Seven Steps to Effectively Defend Industrial Control Systems* at 3.

11. The Commission seeks comment on whether the CIP Reliability Standards should be modified to require isolation between the Internet and BES Cyber Systems in Control Centers performing the functions of a transmission operator. In addition, the Commission seeks comment on the operational impact to the Bulk-Power System if BES Cyber Systems were isolated from the Internet in all Control Centers performing transmission operator functions. Specifically, the Commission seeks comment on what, if any, reliability issues might arise from such a requirement. For example, would requiring isolation prevent an activity required by another Reliability Standard? If isolation is required, is logical isolation preferable to physical isolation (or vice versa) and, if so, why? The Commission also seeks comment on whether and how such a requirement might affect a transmission operator's communications with its reliability coordinator or other applicable entities required under the Reliability Standard. Finally, if isolation is not required, are there communications with these Control Centers for which the use of one-way data diodes would be reliable and appropriate?

B. Application Whitelisting for BES Cyber Systems in Control Centers

12. Application whitelisting is a computer administration practice used to prevent unauthorized programs from running.[13] The purpose is primarily to protect computers and networks from harmful applications, and, to a lesser extent, to prevent unnecessary demand for computer resources. The "whitelist" is a list of applications granted

[13] *See* Alert at Mitigation Section.

permission to run by the user or an administrator. Whitelisting works best when applied to static cyber systems.[14]

13. In response to the Ukraine incident, the Alert recommended that:

> asset owners take defensive measures by leveraging best practices to minimize the risk from similar malicious cyber activity. Application Whitelisting (AWL) can detect and prevent attempted execution of malware uploaded by malicious actors. The static nature of some systems, such as database servers and HMI computers, make these ideal candidates to run AWL. Operators are encouraged to work with their vendors to baseline and calibrate AWL deployments.

Similarly, a December 2015 document by DHS identifies application whitelisting as the first of seven strategies to defend industrial control systems and states that this strategy would have "potentially mitigated" 38 percent of ICS-CERT Fiscal Year 2014 and 2015 incidents, more than any of the other strategies.[15] While the NERC Guidelines and Technical Basis document associated with Reliability Standard CIP-007-6, Requirement R3 identifies application whitelisting as an option for mitigating malicious cyber activity, its use is not mandatory.[16] The Guidelines and Technical Basis discussion in Reliability Standard CIP-007-6 explains:

---

[14] *Id.*

[15] Seven Steps to Effectively Defend Industrial Control Systems at 1.

[16] Reliability Standard CIP-007-6, Requirement R3 provides that "[e]ach Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in CIP-007-6 Table R3 – Malicious Code Prevention" and lists application whitelisting as an option. In addition, the CIP Reliability Standards require a combination of ensuring that an individual's privileges are the minimum necessary to perform their work function (i.e., "least privilege") and anti-

(continued…)

> Due to the wide range of equipment comprising the BES Cyber Systems and the wide variety of vulnerability and capability of that equipment to malware as well as the constantly evolving threat and resultant tools and controls, it is not practical within the standard to prescribe how malware is to be addressed on each Cyber Asset. Rather, the Responsible Entity determines on a BES Cyber System basis, which Cyber Assets have susceptibility to malware intrusions and documents their plans and processes for addressing those risks and provides evidence that they follow those plans and processes. There are numerous options available including traditional antivirus solutions for common operating systems, white-listing solutions, network isolation techniques, Intrusion Detection/Prevention (IDS/IPS) solutions, etc.[17]

14. While application whitelisting is identified above as one available option, the Ukraine incident and the subsequent Alert raise the question of whether application whitelisting should be required. Application whitelisting could be a more effective mitigation tool than other mitigation measures because whitelisting allows only software applications and processes that are reviewed and tested before use in the system network. By knowing all installed applications, the security professional can set the application whitelisting program to know the application is approved; all unapproved applications will trigger an alert.

15. The Commission seeks comment on whether the CIP Reliability Standards should be modified to require application whitelisting for all BES Cyber Systems in Control Centers. Is application whitelisting appropriate for all such systems? If not, are there

---

malware (i.e., "blacklisting"). *See, e.g.*, Reliability Standard CIP-004-6, Requirement R4 and Guidelines and Technical Basis; Reliability Standard CIP-007-6, Requirement R3.

[17] Reliability Standard CIP-007-6, Guidelines and Technical Basis, at 4.

certain devices or components on such systems for which it is appropriate? In addition, the Commission seeks comment on the operational impact, including potential reliability concerns, for each approach.

III. Comment Procedures

16. The Commission invites interested persons to submit comments, and other information on the matters, issues and specific questions identified in this notice. Comments are due **[INSERT DATE that is 60 days from publication in the FEDERAL REGISTER]**. Comments must refer to Docket No. RM16-18-000, and must include the commenter's name, the organization they represent, if applicable, and their address in their comments.

17. The Commission encourages comments to be filed electronically via the eFiling link on the Commission's web site at http://www.ferc.gov. The Commission accepts most standard word processing formats. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format. Commenters filing electronically do not need to make a paper filing.

18. Commenters that are not able to file comments electronically must send an original of their comments to: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street NE, Washington, DC 20426.

19. All comments will be placed in the Commission's public files and may be viewed, printed, or downloaded remotely as described in the Document Availability section

below. Commenters on this proposal are not required to serve copies of their comments on other commenters.

IV. Document Availability

20. In addition to publishing the full text of this document in the Federal Register, the Commission provides all interested persons an opportunity to view and/or print the contents of this document via the Internet through FERC's Home Page (http://www.ferc.gov) and in FERC's Public Reference Room during normal business hours (8:30 a.m. to 5:00 p.m. Eastern time) at 888 First Street, NE, Room 2A, Washington, DC 20426.

21. From FERC's Home Page on the Internet, this information is available on eLibrary. The full text of this document is available on eLibrary in PDF and Microsoft Word format for viewing, printing, and/or downloading. To access this document in eLibrary, type the docket number excluding the last three digits of this document in the docket number field.

22. User assistance is available for eLibrary and the FERC's website during normal business hours from FERC Online Support at 202-502-6652 (toll free at 1-866-208-3676)

or email at ferconlinesupport@ferc.gov, or the Public Reference Room at (202) 502-8371, TTY (202) 502-8659. E-mail the Public Reference Room at public.referenceroom@ferc.gov.

By direction of the Commission.

(S E A L)

Kimberly D. Bose,
Secretary.