161 FERC ¶ 61,291
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket Nos. RM18-2-000 and AD17-9-000]

Cyber Security Incident Reporting Reliability Standards

(Issued December 21, 2017)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Notice of proposed rulemaking.

SUMMARY: The Federal Energy Regulatory Commission (Commission) proposes to direct the North American Electric Reliability Corporation (NERC), the Commission-certified Electric Reliability Organization, to develop and submit modifications to the NERC Reliability Standards to improve mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system.

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

ADDRESSES: Comments, identified by docket number, may be filed in the following ways:

- Electronic Filing through http://www.ferc.gov. Documents created electronically using word processing software should be filed in native applications or print-to-PDF format and not in a scanned format.

- Mail/Hand Delivery: Those unable to file electronically may 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:

Margaret Scott (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6704
margaret.scott@ferc.gov

Kevin Ryan (Legal Information)
Office of the General Counsel
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6840
kevin.ryan@ferc.gov

SUPPLEMENTARY INFORMATION:

161 FERC ¶ 61,291
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

Before Commissioners: Kevin J. McIntyre, Chairman;
Cheryl A. LaFleur, Neil Chatterjee,
Robert F. Powelson, and Richard Glick.

Cyber Security Incident Reporting Reliability Standards Docket Nos. RM18-2-000
AD17-9-000

NOTICE OF PROPOSED RULEMAKING

(Issued December 21, 2017)

1. The Foundation for Resilient Societies filed a petition asking the Commission to require additional measures for malware detection, mitigation, removal and reporting. We decline to propose additional Reliability Standard measures at this time for malware detection, mitigation and removal, based on the scope of existing Reliability Standards, Commission-directed improvements already being developed and other ongoing efforts. However, we propose to direct broader reporting requirements. Currently, incidents must be reported only if they have "compromised or disrupted one or more reliability tasks," and we propose to require reporting of certain incidents even before they have caused such harm or if they did not themselves cause any harm.

2. Specifically, pursuant to section 215(d)(5) of the Federal Power Act (FPA),[1] the Commission proposes to direct the North American Electric Reliability Corporation

[1] 16 U.S.C. 824o(d)(5).

(NERC), the Commission-certified Electric Reliability Organization (ERO), to develop and submit modifications to the Critical Infrastructure Protection (CIP) Reliability Standards to improve the reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system. The proposed development of modified mandatory reporting requirements is intended to improve awareness of existing and future cyber security threats and potential vulnerabilities. We propose to continue having the reports go to the Electricity Information Sharing and Analysis Center (E-ISAC) instead of the Commission, but we propose to require that reports also be sent to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and that NERC file an annual, public, and anonymized summary of the reports.

3. The current reporting threshold for Cyber Security Incidents, as set forth in Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning) together with the definition of Reportable Cyber Security Incident, may understate the true scope of cyber-related threats facing the Bulk-Power System. The reporting of cyber-related incidents, in particular the lack of any reported incidents in 2015 and 2016, suggests a gap in the current mandatory reporting requirements. This reporting gap may result in a lack of timely awareness for responsible entities subject to compliance with the CIP Reliability Standards, NERC, and the Commission. As discussed below, NERC's 2017 State of Reliability report echoed this concern in stating

that the "mandatory reporting process does not create an accurate picture of cyber security risk…"[2]

4. To address this gap, pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct NERC to develop modifications to the CIP Reliability Standards to include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).[3] Such modifications will enhance awareness for NERC, industry, the Commission, other federal and state entities, and interested stakeholders regarding existing or developing cyber security threats. In addition, we propose to direct NERC to modify the CIP Reliability Standards to specify the required information in Cyber Security Incident reports to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information. Finally, we propose to direct NERC to modify the CIP Reliability Standards to establish a deadline for filing a report once a compromise or

[2] NERC, 2017 State of Reliability Report at 4 (June 2017), http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MASTER_20170613.pdf.

[3] The NERC Glossary of Terms Used in NERC Reliability Standards (October 6, 2017) (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."

disruption to reliable bulk electric system operation, or an attempted compromise or disruption, is identified by a responsible entity.

I. Background

A. Section 215 and Mandatory Reliability Standards

5. Section 215 of the FPA requires a Commission-certified ERO to develop mandatory and enforceable Reliability Standards, subject to Commission review and approval. Reliability Standards may be enforced by the ERO, subject to Commission oversight, or by the Commission independently.[4] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[5] and subsequently certified NERC.[6]

B. Foundation for Resilient Societies' Petition

6. On January 13, 2017, the Foundation for Resilient Societies (Resilient Societies) filed a petition requesting that the Commission initiate a rulemaking to require an enhanced Reliability Standard for malware detection, reporting, mitigation and removal from the Bulk-Power System.[7] Resilient Societies stated that the Bulk-Power System is

[4] 16 U.S.C. 824o(e).

[5] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards*, Order No. 672, FERC Stats. & Regs. ¶ 31,204 (cross-referenced at 114 FERC ¶ 61,104), *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (cross-referenced at 114 FERC ¶ 61,328) (2006).

[6] *North American Electric Reliability Corp.*, 116 FERC ¶ 61,062, *order on reh'g and compliance*, 117 FERC ¶ 61,126 (2006), *aff'd sub nom. Alcoa, Inc. v. FERC*, 564 F.3d 1342 (D.C. Cir. 2009).

[7] Resilient Societies' filings and responsive comments are available on the Commission's eLibrary document retrieval system in Docket No. AD17-9-000.

increasingly at risk from malware. Resilient Societies also maintained that current mandatory and voluntary reporting methods underreport the actual annual rate of occurrence of cybersecurity incidents in the U.S. electric grid.

7. In support of its petition, Resilient Societies asserted that evidence in the public domain shows that electric grids in the U.S. and critical infrastructure that depends upon reliable power are increasingly at risk from malware, resulting in a threat of widespread, long-term blackouts. Resilient Societies asserted that Bulk-Power System assets are interconnected with the public internet, which could allow foreign adversaries to implant malware in electric utility computer systems. Resilient Societies stated that malware can infect high, medium, and low impact BES Cyber Systems,[8] and, once inserted, can be a pathway for cyber-attackers.[9] Resilient Societies further stated that an infected low impact BES Cyber System can serve as an entry point from where an adversary can attack medium and high impact BES Cyber Systems. Resilient Societies asserted that a "simultaneous cyberattack on many low impact assets may cause greater impact than an attack on a single high impact asset."[10]

[8] Reliability Standard CIP-002-5.1a (Cyber Security System Categorization) provides a "tiered" approach to cybersecurity requirements, based on classifications of high, medium and low impact BES Cyber Systems.

[9] BES Cyber System is defined by NERC as "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity." NERC Glossary. The acronym BES refers to the bulk electric system.

[10] Resilient Societies Petition at 2-3.

8. Resilient Societies alleged that it has found gaps relating to malware protection requirements in the current Commission-approved CIP Reliability Standards. In particular, Resilient Societies maintained that the ESP concept, used in the CIP Reliability Standards, suffers from several fundamental flaws. Specifically, Resilient Societies asserted that: (1) cyber attacks on systems outside the ESP can take down systems within it; (2) passwords and other user credentials associated with BES Cyber Systems may be stored on systems outside the ESP; and (3) Electronic Access Points that control access to systems within the ESP may be breached. Resilient Societies also raised a concern that there is currently no required reporting of malware infections, both inside and outside the ESP.[11]

9. Based on its analysis, Resilient Societies offered several suggestions for the essential components of an enhanced malware Reliability Standard and what the technical elements of an enhanced malware standard might include. The essentials identified by Resilient Societies include: (1) malware detection; (2) malware reporting (regardless of whether reliability tasks of a functional entity have been compromised or disrupted); (3) malware mitigation; and (4) mandatory malware removal. Resilient

[11] *Id.* at 10-12.

Societies also provided a list of possible technical elements for an enhanced malware Reliability Standard.[12]

10. In support of its request for an enhanced Reliability Standard for malware reporting, Resilient Societies asserted that current mandatory and voluntary cybersecurity incident reporting methodologies are not representative of the actual annual rate of occurrence of cybersecurity incidents in the U.S. electric grid. Resilient Societies cited NERC's State of Reliability Reports for 2014 and 2015, noting that NERC identified only three Reportable Cyber Security Incidents in 2014 and zero Reportable Cyber Security Incidents in 2015. In addition, Resilient Societies observed that according to Department of Energy (DOE) Disturbance Reports (OE-417), there were three reported cybersecurity incidents in 2014, zero in 2015, and two in 2016. Finally, Resilient Societies stated that in contrast to the number of cybersecurity incidents reported through NERC and DOE Form OE-417, ICS-CERT responded to 79 cybersecurity incidents in 2014 and 46 cybersecurity incidents in 2015.[13]

11. On February 17, 2017, Resilient Societies filed supplemental comments that included an appendix containing a February 10, 2017 Department of Homeland Security (DHS) Report, "Enhanced Analysis of GRIZZLY STEPPE Activity," which, Resilient Societies alleged, "provides independent validation of the need for a mandatory standard

[12] *Id.* at 14-15.

[13] *Id.* at 8-9.

to detect, report, mitigate, and remove identified malware from the Bulk Power System."[14]

Comments on Petition

12. The Commission received five sets of comments in response to Resilient Societies' petition. Among the commenters, NERC, Trade Associations[15] and International Transmission Company (ITC) stated that the Commission should not act on Resilient Societies' petition, claiming that the issues raised therein are adequately addressed in the currently-effective CIP Reliability Standards or are, in response to outstanding Commission directives, the subject of ongoing standards projects. The other two commenters, Kaspersky Lab, and David Bardin, supported Resilient Societies' petition to better address the detection, reporting and mitigation of malware.

13. NERC opposed Resilient Societies' petition because, NERC asserted, existing CIP Reliability Standards, current standard development activity and other cyber security efforts adequately address the threats, vulnerabilities and risks associated with malware detailed in the Resilient Societies' petition. Accordingly, NERC concluded that a new Reliability Standard to address malware detection, reporting, mitigation and removal is

[14] Resilient Societies Supplemental Comments at 4.

[15] American Public Power Association, Edison Electric Institute, Electricity Consumers Resource Council, Electric Power Supply Association, Large Public Power Council, National Rural Electric Cooperative Association, and Transmission Access Policy Study Group.

not necessary at this time.[16] With regard to the Commission-approved CIP Reliability Standards, NERC stated that several existing requirements require responsible entities to implement protections to address the threat of malware.[17] NERC identified seven currently-effective CIP requirements that it alleged address the risks associated with malware.[18]

14. With regard to current standard development activity, NERC observed that modifications to the CIP Reliability Standards being developed in response to Commission Order Nos. 822 and 829 will further mitigate the risks posed by malware.[19] Specifically, NERC stated that the modifications under development in response to Order No. 822 address malware protections for assets containing low impact BES Cyber Systems and protections for communication links and sensitive data communicated between bulk electric system control centers. In particular, NERC identified proposed Reliability Standard CIP-003-7 and stated that the proposed Reliability Standard clarifies

[16] NERC Comments at 1-2.

[17] *Id.* at 2.

[18] *Id.* at 5-6.

[19] *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 822, 154 FERC ¶ 61,037, *reh'g denied,* Order No. 822-A, 156 FERC ¶ 61,052 (2016); *Revised Critical Infrastructure Protection Reliability Standards*, Order No. 829, 156 FERC ¶ 61,050 (2016).

electronic access controls and mitigates the introduction of malicious code from transient devices for assets containing low impact BES Cyber Systems.[20]

15. NERC stated that proposed Reliability Standard CIP-013-1 (Cyber Security - Supply Chain Risk Management), developed in response to Order No. 829, requires responsible entities to, among other things, implement at least one process to verify the integrity and authenticity of certain software and firmware and implement at least one process to control vendor remote access to high and medium impact BES Cyber Systems.[21] For low impact BES Cyber Systems, NERC explained that the proposed Reliability Standard requires responsible entities to have at least one cyber security policy that addresses integrity and authenticity of software and hardware and to adopt controls for vendor-initiated remote access. NERC states that this proposed Reliability Standard

[20] NERC Comments at 8. On October 19, 2017, the Commission issued a notice of proposed rulemaking proposing to approve proposed Reliability Standard CIP-003-7. *See Revised Critical Infrastructure Protection Reliability Standard CIP-003-7 – Cyber Security – Security Management Controls*, Notice of Proposed Rulemaking, 82 Fed. Reg. 49,541 (October 26, 2017), 161 FERC ¶ 61,047 (2017).

[21] On September 26, 2017, NERC submitted proposed Reliability Standards CIP-013-1, CIP-005-6 and CIP-010-3 for Commission approval. NERC's filing is available on the Commission's eLibrary document retrieval system in Docket No. RM17-13-000 and on the NERC website, www.nerc.com.

shows NERC and industry "are taking significant steps in addressing the risks posed by malware campaigns targeting supply chain vendors."[22]

16. With regard to other ongoing cyber security efforts, NERC noted the activities of the E-ISAC. Specifically, NERC stated that, through the E-ISAC, NERC has "fostered an information sharing culture that promotes a proactive approach towards identification of malware, pooling of resources to combat malware, and sharing of best practices based on lessons learned, among other things."[23] In addition, NERC maintained that it facilitates industry information sharing in two other ways: NERC Alerts and the activities of the Critical Infrastructure Protection Committee (CIPC). NERC concluded that these activities promote necessary information sharing of cyber security threats and help foster the type of incident reporting requested in Resilient Societies' petition.[24]

17. While acknowledging the validity of concerns regarding the threat malware poses to the bulk electric system, ITC asserted that Resilient Societies' conclusion that existing CIP Reliability Standards contain gaps with respect to malware defense is inaccurate. ITC stated that, contrary to Resilient Societies' conclusions, the lack of specific malware-related controls in the CIP Reliability Standards "reflects a critically important objectives-based approach which the Commission has intentionally adopted."[25] ITC

---

[22] NERC Comments at 9.

[23] *Id.*

[24] *Id.* at 12-13.

[25] ITC Comments at 2-3.

explained that the existing CIP Reliability Standards "collectively mandate robust and effective malware security measures, through both direct security measures that thwart malware attacks, and through complementary measures, such as personnel training against social engineering attacks."[26] ITC concluded that the specific controls in Resilient Societies' requests that the Commission mandate are duplicative, unnecessary and/or overly and unreasonably burdensome, and would make the bulk electric system less reliable and more vulnerable compared to the existing protections.[27]

18. Trade Associations stated that the risks raised in Resilient Societies' petition are addressed under the current CIP Reliability Standards and in ongoing Commission dockets and standards development efforts. Trade Associations observed that Reliability Standard CIP-007-6, Requirement R3 is the primary existing Reliability Standard addressing the risks posed by malware. Trade Associations explained that the Reliability Standard requires responsible entities to deter, detect, or prevent malicious code; mitigate the threat of detected malicious code; and have a process to update signatures or patterns associated with malicious code. Trade Associations asserted that other relevant requirements are spread throughout the currently-effective CIP Reliability Standards, including Reliability Standards CIP-005-5, Requirement R1 (Electronic Security Perimeter); CIP-005-5, Requirement R2 (Protections for Interactive Remote Access);

[26] *Id.* at 3.

[27] *Id.* at 2-3.

CIP-007-6, Requirement R1 (limiting and protecting accessible ports); and CIP-007-6, Requirement R2 (patch management required to detect software vulnerabilities).[28]

19. In addition, Trade Associations noted recently-approved new CIP Reliability Standards addressing transient devices associated with high and medium impact BES Cyber Systems, as well as the Commission's directive in Order No. 822 for the development of similar protections for low impact BES Cyber Systems. Trade Associations also identified the Commission's directives in Order No. 829 relating to cybersecurity risks posed by vendors as open initiatives that will help protect against the introduction of malware into BES Cyber Systems.[29]

20. Kaspersky Lab supported the development of an enhanced Reliability Standard for malware detection, reporting, mitigation and removal. Kaspersky Lab stated that the current CIP Reliability Standards "do not sufficiently address malware protection as a critical component in securing BES Cyber Assets and Systems."[30] Kaspersky Lab offered a list of reasons why it believes that electric utilities face an increased risk of being infiltrated by malware, highlighting, among other issues, that information concerning exploitable vulnerabilities is increasingly becoming public. Kaspersky Lab noted that it recognizes that the CIP Reliability Standards "strive to address the complex cyber and physical security needs of the [bulk electric system]" and that cybersecurity standards "must be flexible and not overly prescriptive to address threats as they evolve,"

[28] Trade Associations Comments at 5-6.

[29] *Id.* at 7.

[30] Kaspersky Lab Comments at 1.

but it states that the current CIP Reliability Standards only address malware protection "in a cursory fashion."[31]

21. David Bardin supported the goals in Resilient Societies' petition and suggested that the Commission initiate one or more proceedings to facilitate a conversation on malware protections. In support of his position, Bardin presented a list of questions that could be raised in such discussions.[32]

C. NERC 2017 State of Reliability Report

22. In June 2017, NERC published the 2017 NERC State of Reliability Report which, among other things, indicates that there were no Reportable Cyber Security Incidents in 2016. The report also lists "key findings" regarding reliability performance observed over the previous year and recommendations for improvements. Key Finding 4 of the report addresses the reporting of Cyber Security Incidents. In particular, NERC states that the current "mandatory reporting process does not create an accurate picture of cyber security risk since most of the cyber threats detected by the electricity industry manifest themselves in … email, websites, smart phone applications … rather than the control system environment where impacts could cause loss of load and result in a mandatory report."[33] Based on that finding, the report includes a recommendation that NERC and

[31] *Id.* at 2.

[32] Bardin Comments at 1.

[33] 2017 NERC State of Reliability Report at 4.

industry should "redefine reportable incidents to be more granular and include zero-consequence incidents that might be precursors to something more serious."[34]

II. Discussion

23. Pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct NERC to develop modifications to the CIP Reliability Standards to address the Commission's concerns regarding mandatory reporting requirements. Based on our review of the comments received in response to Resilient Societies' petition, however, we conclude that the current Commission-approved CIP Reliability Standards, ongoing NERC efforts to address open Commission directives, and other industry efforts have addressed or will address the malware detection and mitigation issues raised by Resilient Societies. For example, provisions of currently effective Reliability Standards, including CIP-005-5 and CIP-007-6, address malware detection and mitigation. Ongoing efforts described by NERC and other commenters, such as the development of a supply chain risk management standard, should also address malware concerns. Thus, the Commission declines to act on this aspect of the petition.[35]

24. We believe that the current reporting threshold for Cyber Security Incidents, as set forth in the current definition of Reportable Cyber Security Incident, may not reflect the true scope of cyber-related threats facing the Bulk-Power System, consistent with

[34] *Id.*

[35] While the Commission proposes that NERC develop modifications to the NERC Reliability Standards under section 215(d)(5) of the FPA in Docket No. RM18-2-000, we exercise our discretion to terminate the proceeding in Docket No. AD17-9-000.

NERC's view. Accordingly, pursuant to section 215(d)(5) of the FPA, the Commission proposes to direct that NERC develop modifications to the CIP Reliability Standards to improve the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system, to improve awareness of existing and future cyber security threats and potential vulnerabilities.

25. Below, we discuss the following elements of the proposed directive: (A) Cyber Security Incident reporting threshold; (B) information in Cyber Security Incident reports; and (C) timing of Cyber Security Incident reports.

A. Cyber Security Incident Reporting Threshold

26. Cyber-related event reporting is currently addressed in Reliability Standard CIP-008-5, Requirement R1, Part 1.2, which requires that each responsible entity shall document one or more Cyber Security Incident Plan(s) with one or more processes to determine if an identified Cyber Security Incident is a Reportable Cyber Security Incident. Where a cyber-related event is determined to qualify as a Reportable Cyber Security Incident, responsible entities are required to notify the E-ISAC with initial notification to be made within one hour from the determination of a Reportable Cyber Security Incident.[36]

[36] *See* Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning), Requirement R1, Part 1.2. This requirement pertains to high impact BES Cyber Systems and medium impact BES Cyber Systems.

27. A Cyber Security Incident is defined in the NERC Glossary as:

> A malicious act or suspicious event that:
> • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or,
> • Disrupts, or was an attempt to disrupt, the operation of a BES Cyber System.

This is similar, but not identical, to the definition of a cybersecurity incident in FPA section 215, which is "a malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communication networks including hardware, software and data that are essential to the reliable operation of the bulk power system."[37] A Reportable Cyber Security Incident, however, is defined more narrowly in the NERC Glossary as "[a] Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." Therefore, in order for a cyber-related event to be considered reportable under the existing CIP Reliability Standards, it must compromise or disrupt a core activity (e.g., a reliability task) of a responsible entity that is intended to maintain bulk electric system reliability.[38] Under these definitions, unsuccessful attempts to compromise or disrupt a responsible

[37] 16 U.S.C. 824o(a)(8).

[38] The NERC Functional Model "describes a set of Functions that are performed to ensure the reliability of the Bulk Electric System. Each Function consists of a set of related reliability Tasks. The Model assigns each Function to a functional entity, that is, the entity that performs the function. The Model also describes the interrelationships between that functional entity and other functional entities (that perform other Functions)." NERC, Reliability Functional Model: Function Definitions and Functional Entities, Version 5 at 7 (November 2009), http://www.nerc.com/pa/Stand/Functional%20Model%20Archive%201/Functional_Model_V5_Final_2009Dec1.pdf.

entity's core activities are not subject to the current reporting requirements in Reliability Standard CIP-008-5.

28. As discussed above, recent NERC State of Reliability Reports indicate that there were no Reportable Cyber Security Incidents in 2015 and 2016. As noted by NERC, "[w]hile there were no reportable cyber security incidents during 2016 and therefore none that caused a loss of load, this does not necessarily suggest that the risk of a cyber security incident is low."[39] In contrast, the 2016 annual summary of DOE's Electric Disturbance Reporting Form OE-417 contained four cybersecurity incidents reported in 2016: two suspected cyber attacks and two actual cyber attacks.[40] Moreover, ICS-CERT responded to fifty-nine cybersecurity incidents within the Energy Sector in 2016.[41]

29. Based on this comparison, the current reporting threshold in Reliability Standard CIP-008-5 may not reflect the true scope and scale of cyber-related threats facing responsible entities. The disparity in the reporting of cyber-related incidents under existing reporting requirements, in particular the lack of any incidents reported to NERC in 2015 and 2016, suggests a gap in the current reporting requirements. We are concerned that this apparent reporting gap results in a lack of awareness for NERC,

---

[39] 2017 NERC State of Reliability Report at 4.

[40] 2016 DOE Electric Disturbance Events (OE-417) Annual Summary Archives, https://www.oe.netl.doe.gov/OE417_annual_summary.aspx.

[41] ICS-CERT cybersecurity incident statistics for the Energy Sector combine statistics from the electric subsector and the oil and natural gas subsector. ICS-CERT does not break out the cybersecurity incidents that only impact the electric subsector. 2016 ICS-CERT Year in Review, https://ics-cert.us-cert.gov/Year-Review-2016.

responsible entities, and the Commission. This concern is echoed in the 2017 NERC State of Reliability Report, which includes a recommendation that NERC and industry should "redefine reportable incidents to be more granular and include zero-consequence incidents that might be precursors to something more serious."[42] We agree with NERC's recommendation. The disparity highlights the need to improve the reporting obligation under the CIP Reliability Standards.

30. The Commission proposes to direct NERC to address the gap in cyber-related incident reporting. Specifically, we propose to direct NERC to modify the CIP Reliability Standards to include the mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS. Enhanced mandatory reporting of cyber-related incidents will provide better awareness to NERC, industry and the Commission regarding existing or developing cyber security threats.

31. Reporting of attempts to compromise, instead of only successful compromises, is consistent with current monitoring requirements. For example, Reliability Standard CIP-007-6, Requirement R4.1, mandates logging of detected successful login attempts, detected failed access attempts, and failed login attempts. Also, the Guidelines and

[42] 2017 NERC State of Reliability Report at 4.

Technical Basis for this requirement state that events should be logged even if access attempts were blocked or otherwise unsuccessful.[43]

32. Similarly, DHS defines a "cyber incident" as "attempts (either failed or successful) to gain unauthorized access to a system or its data…."[44] The E-ISAC defines a "cyber incident" as including unauthorized access through the electronic perimeter as well as "a detected effort … without obvious success."[45] Also, ICS-CERT defines a "cyber incident" as an "occurrence that actually or potentially results in adverse consequences…."[46]

33. We propose to establish a compromise or an attempt to compromise a responsible entity's ESP or associated EACMS, due to their close association with ESPs, as the boundary point for a reportable Cyber Security Incident. An ESP is defined in the NERC Glossary as the "logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol." The purpose of an ESP is to manage electronic access to BES Cyber Systems to support the protection of the BES Cyber Systems against

---

[43] *See* Reliability Standard CIP-007-6 (Cyber Security – Systems Security Management), Requirement R4, Part 1.

[44] *See* United States Computer Emergency Readiness Team (US-CERT) Incident Definition: https://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition.

[45] *See* E-ISAC Incident Reporting Fact Sheet document: http://www.nerc.com/files/Incident-Reporting.pdf.

[46] *See* ICS-CERT Published "Common Cyber Security Language" document: https://ics-cert.us-cert.gov/About-Industrial-Control-Systems-Cyber-Emergency-Response-Team

compromise that could lead to misoperation or instability in the bulk electric system.[47] EACMS are defined in the NERC Glossary 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." More specifically, EACMS include, for example, firewalls, authentication servers, security event monitoring systems, intrusion detection systems and alerting systems.[48] Therefore, EACMS control electronic access into the ESP and play a significant role in the protection of high and medium impact BES Cyber Systems.[49] Once an EACMS is compromised, an attacker could more easily enter the ESP and effectively control the BES Cyber System or Protected Cyber Asset.

34. Since an ESP is intended to protect BES Cyber Systems and EACMS are intended to control electronic access into an ESP, we believe it is reasonable to establish the compromise of, or attempt to compromise, an ESP or its associated EACMS as the minimum reporting threshold.

---

[47] *See* Reliability Standard CIP-005-5 (Cyber Security – Electronic Security Perimeter(s)).

[48] *See* Reliability Standard CIP-002-5.1 (Cyber Security – BES Cyber System Categorization), Background at 6; Reliability Standard CIP-007-6 (Cyber Security – System Security Management), Background at 4.

[49] *See* Reliability Standard CIP-002-5.1a (Cyber Security – BES Cyber System Categorization), Background at 5-6 ("BES Cyber Systems have associated Cyber Assets, which, if compromised, pose a threat to the BES Cyber System by virtue of: (a) their location within the Electronic Security Perimeter (Protected Cyber Assets), or (b) the security control function they perform (Electronic Access Control or Monitoring Systems and Physical Access Control Systems").

35. In sum, pursuant to section 215(d)(5) of the FPA, we propose to direct NERC to develop modifications to the CIP Reliability Standards described above to improve the reporting of Cyber Security Incidents, including incidents that did not cause any harm but could facilitate subsequent efforts to harm the reliable operation of the bulk electric system. The Commission seeks comment on this proposal.

36. In addition, the Commission seeks comment on whether to exclude EACMS from any Commission directive and, instead, establish the compromise, or attempt to compromise, an ESP as the minimum reporting threshold. The Commission also seeks comment on potential alternatives to modifying the mandatory reporting requirements in the NERC Reliability Standards. Specifically, we seek comment on whether a request for data or information pursuant to Section 1600 of the NERC Rules of Procedure would effectively address the reporting gap and current lack of awareness of cyber-related incidents, discussed above, among NERC, responsible entities and the Commission, and satisfy the goals of the proposed directive.

B. Content of Cyber Security Incident Reports

37. Currently-effective Reliability Standard CIP-008-5, Requirement R1, Part 1.2 requires that a responsible entity provide an initial notification of a Reportable Cyber Security Incident to the E-ISAC within one hour of the determination that a Cyber Security Incident is reportable, unless prohibited by law. The initial notification may be

made by phone call, e-mail, or through a Web-based notice.[50] Reliability Standard CIP-008-5 does not specify the content of a report.

38. The Commission proposes to direct that NERC modify the CIP Reliability Standards to specify the required content in a Cyber Security Incident report. We propose that the minimum set of attributes to be reported should include: (1) the functional impact, when identifiable, 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 as a result of the Cyber Security Incident. Knowledge of these attributes regarding a specific Cyber Security Incident will improve awareness of cyber threats to bulk electric system reliability. These attributes are the same as attributes already used by DHS for its multi-sector reporting and summarized by DHS in an annual report.[51] Specifying the required content should improve the quality of reporting by ensuring that basic information is provided and allows for ease of comparison across reports by ensuring that each report includes specified fields of information.

39. Functional impact is a measure of the actual, ongoing impact to the organization, the affected BES Cyber System(s), and the responsible entity's ability to protect and/or operate the affected BES Cyber System(s) to ensure reliable bulk electric system

[50] *See* Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning), Guidelines and Technical Basis at 19.

[51] 2016 ICS-CERT Year in Review, https://ics-cert.us-cert.gov/Year-Review-2016.

operations. In many cases, such as scans and probes by attackers or a successfully defended attack, there is little or no impact on the responsible entity as a result of the incident. The attack vector is the method used by the attacker to exploit a vulnerability, such as a phishing attack for user credentials or a virus designed to exploit a known vulnerability. The level of intrusion reflects the extent of the penetration into a responsible entity's ESP, EACMS as applicable, or BES Cyber Systems within the ESP, that was achieved as a result of the Cyber Security Incident.

40. The Commission seeks comment on this proposal and, more generally, the appropriate content for Cyber Security Incident reporting to improve awareness of existing and future cyber security threats and potential vulnerabilities.

C. Timing of Cyber Security Incident Reports

41. In addition to addressing the specific content for Cyber Security Incident reports, the Commission proposes that NERC establish requirements outlining deadlines for filing a report once a compromise or disruption to reliable bulk electric system operation, or an attempted compromise or disruption, is identified by a responsible entity. While currently-effective Reliability Standard CIP-008-5, Requirement R1, Part 1.2 requires that a responsible entity provide an initial notification of a Reportable Cyber Security Incident to the E-ISAC within one hour of the determination that a Cyber Security Incident is reportable, unless prohibited by law, the Reliability Standard "does not require a specific timeframe for completing the full report."[52] The reporting timeline should

[52] *See* Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning), Guidelines and Technical Basis at 19.

reflect the actual or potential threat to reliability, with more serious incidents reported in a more timely fashion. A reporting timeline that takes into consideration the severity of a Cyber Security Incident should minimize potential burdens on responsible entities. The intent of this directive is to provide NERC with the information necessary to maintain awareness regarding cyber threats to bulk electric system reliability. We propose that the reports submitted under the enhanced mandatory reporting requirements would be provided to E-ISAC, similar to the current reporting scheme, as well as ICS-CERT. The detailed incident reporting would not be submitted to the Commission.

42. The Commission and others will also benefit from enhanced Cyber Security Incident reporting as we continue to evaluate the effectiveness of the CIP Reliability Standards. Currently, NERC identifies the number of Reportable Cyber Security Incidents in its annual State of Reliability report. In that regard, however, we propose to direct NERC to file publicly an annual report reflecting the Cyber Security Incidents reported to NERC during the previous year. Specifically, we propose to direct NERC to file annually an anonymized report providing an aggregated summary of the reported information. We believe that the ICS-CERT annual report, which includes pie charts reflecting the energy sector's cybersecurity incidents by level of intrusion, threat vector and functional impact, would be a reasonable model for what NERC reports to the Commission.[53]

[53] ICS-CERT, https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_IR_Pie_Chart_FY2016_S508C.pdf.

43. The Commission seeks comment on the appropriate timing for Cyber Security Incident reporting to better ensure timely sharing of information and thereby enhance situational awareness. In addition, the Commission seeks comment on the proposal to direct NERC to file an annual report with the Commission.

III. Information Collection Statement

44. The Paperwork Reduction Act (PRA) requires each federal agency to seek and obtain approval from the Office of Management and Budget (OMB) before undertaking a collection of information directed to ten or more persons, or contained in a rule of general applicability. OMB's implementing regulations require approval of certain information collection requirements imposed by agency rules.[54] Upon approval of a collection(s) of information, OMB will assign an OMB control number and an expiration date. Respondents subject to the filing requirements of an agency rule will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number.

45. The Commission is submitting these proposed reporting requirements to OMB for its review and approval under section 3507(d) of the PRA. Comments are solicited on the Commission's need for the information proposed to be reported, whether the information will have practical utility, ways to enhance the quality, utility, and clarity of the information to be collected, and any suggested methods for minimizing the respondent's burden, including the use of automated information techniques.

[54] *See* 5 CFR 1320.

46. The Public Reporting Burden and cost related to the proposed rule in Docket No. RM18-2-000 are covered by, and already included in, the existing FERC-725, Certification of Electric Reliability Organization; Procedures for Electric Reliability Standards (OMB Control No. 1902-0225). FERC-725 includes the ERO's overall responsibility for developing Reliability Standards, such as any Reliability Standards that relate to Cyber Security Incident reporting.

47. Internal review: The Commission has reviewed the proposed changes and has determined that the changes are necessary to ensure the reliability and integrity of the Nation's Bulk-Power System.

48. Interested persons may obtain information on the reporting requirements by contacting: Federal Energy Regulatory Commission, 888 First Street, NE, Washington, DC 20426 [Attention: Ellen Brown, Office of the Executive Director, e-mail: DataClearance@ferc.gov, Phone: (202) 502-8663, fax: (202) 273-0873]. Comments on the requirements of this rule may also be sent to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission]. For security reasons, comments should be sent by e-mail to OMB at oira_submission@omb.eop.gov. Please refer to OMB Control No. 1902-0225 and FERC-725 in your submission.

IV. Environmental Analysis

49. The Commission is required to prepare an Environmental Assessment or an Environmental Impact Statement for any action that may have a significant adverse effect

on the human environment.[55] The Commission has categorically excluded certain actions from this requirement as not having a significant effect on the human environment. Included in the exclusion are rules that are clarifying, corrective, or procedural or that do not substantially change the effect of the regulations being amended.[56] The actions proposed herein fall within this categorical exclusion in the Commission's regulations.

V. Regulatory Flexibility Act Analysis

50. The Regulatory Flexibility Act of 1980 (RFA)[57] generally requires a description and analysis of proposed rules that will have significant economic impact on a substantial number of small entities.

51. By only proposing to direct NERC, the Commission-certified ERO, to develop modified Reliability Standards for Cyber Security Incident reporting, this Notice of Proposed Rulemaking will not have a significant or substantial impact on entities other than NERC. Therefore, the Commission certifies that this Notice of Proposed Rulemaking will not have a significant economic impact on a substantial number of small entities.

52. Any Reliability Standards proposed by NERC in compliance with this rulemaking will be considered by the Commission in future proceedings. As part of any future

[55] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987) (cross-referenced at 41 FERC ¶ 61,284).

[56] 18 CFR 380.4(a)(2)(ii).

[57] 5 U.S.C. 601-612.

proceedings, the Commission will make determinations pertaining to the Regulatory Flexibility Act based on the content of the Reliability Standards proposed by NERC.

VI. Comment Procedures

53. The Commission invites interested persons to submit comments on the matters and issues proposed in this notice to be adopted, including any related matters or alternative proposals that commenters may wish to discuss. Comments are due [**INSERT DATE 60 days after publication in the FEDERAL REGISTER**]. Comments must refer to Docket No. RM18-2-000, and must include the commenter's name, the organization they represent, if applicable, and address.

54. 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.

55. 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.

56. 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.

VII. Document Availability

57. 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 the Commission's Home Page (http://www.ferc.gov) and in the Commission'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.

58. From the Commission'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 of this document, excluding the last three digits, in the docket number field.

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

Nathaniel J. Davis, Sr.,
Deputy Secretary.