164 FERC ¶ 61,033
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM18-2-000; Order No. 848]

Cyber Security Incident Reporting Reliability Standards

(Issued July 19, 2018)

AGENCY: Federal Energy Regulatory Commission.

ACTION: Final rule.

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

DATES: This rule will become effective **[INSERT DATE 60 days after publication in the FEDERAL REGISTER].**

FOR FURTHER INFORMATION CONTACT:

Margaret Steiner (Technical Information)
Office of Electric Reliability
Federal Energy Regulatory Commission
888 First Street, NE
Washington, DC 20426
(202) 502-6704
Margaret.Steiner@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:

164 FERC ¶ 61,033
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 No. RM18-2-000

ORDER NO. 848

FINAL RULE

(Issued July 19, 2018)

1. Pursuant to section 215(d)(5) of the Federal Power Act (FPA), the Commission directs the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES.[1] The Commission directs NERC to develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible

[1] 16 U.S.C. 824o(d)(5). The NERC Glossary of Terms Used in NERC Reliability Standards (June 12, 2018) (NERC Glossary) defines a Cyber Security Incident 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."

entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).[2]

2. In the NOPR, the Commission observed that Cyber Security Incidents are presently reported by responsible entities in accordance with Reliability Standard CIP-008-5 (Cyber Security – Incident Reporting and Response Planning).[3] However, under the definition of Reportable Cyber Security Incident in Reliability Standard CIP-008-5, responsible entities must only report Cyber Security Incidents if they have "compromised or disrupted one or more reliability tasks." The Commission explained that the current reporting threshold may understate the true scope of cyber-related threats facing the Bulk-Power System, particularly given the lack of any reportable incidents in 2015 and 2016. To improve awareness of existing and future cyber security threats and potential vulnerabilities, the Commission proposed to direct that NERC develop and submit modifications to the existing Reliability Standards to augment the reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES.

3. As discussed in detail below, the Commission adopts the NOPR proposal. The Commission's directive in this Final Rule consists of four elements intended to augment

[2] 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."

[3] *Cyber Security Incident Reporting Reliability Standards*, Notice of Proposed Rulemaking, 82 FR 61,499 (Dec. 28, 2017), 161 FERC ¶ 61,291, P 1 (2017) (NOPR).

the current Cyber Security Incident reporting requirement: (1) responsible entities must report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; (2) required information in Cyber Security Incident reports should include certain minimum information to improve the quality of reporting and allow for ease of comparison by ensuring that each report includes specified fields of information; (3) filing deadlines for Cyber Security Incident reports should be established once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity; 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, NERC must file an annual, public, and anonymized summary of the reports with the Commission.

4. As discussed below, after considering the comments submitted in response to the NOPR, we conclude that the proposed directive to augment the current reporting requirement for Cyber Security Incidents is appropriate to carry out FPA section 215. As NERC recognizes in its NOPR comments, "[b]roadening the mandatory reporting of Cyber Security Incidents would help enhance awareness of cyber security risks facing entities[,] … would create a more extensive baseline understanding of the nature of cyber security threats and vulnerabilities[,] … [and] is consistent with recommendations in

NERC's 2017 State of Reliability Report."[4] Our directive is intended to result in a measured broadening of the existing reporting requirement in Reliability Standard CIP-008-5, consistent with NERC's recommendation, rather than a wholesale change in cyber incident reporting that supplants or otherwise chills voluntary reporting, as some commenters maintain. Indeed, as NERC contends, we believe that the new "baseline understanding, coupled with the additional context from voluntary reports received by the E-ISAC, [will] allow NERC and the E-ISAC to share that information broadly through the electric industry to better prepare entities to protect their critical infrastructure."[5]

5. We address in the discussion below concerns raised by commenters regarding elements of the Commission's directive and the burdens the directive might impose if NERC develops requirements that are overly broad. At the outset, we agree with NERC that "because certain requirements in the CIP Reliability Standards already require entities to track data on compromises or attempts to compromise the ESP or EACMS, the additional burden to report that data appears reasonable."[6] And we do not believe that complying with the augmented reporting requirements that we direct here would be any more burdensome to industry than the alternative, responding to a perpetual data or information request to collect the same information pursuant to Section 1600 of the NERC Rules of Procedure. To ensure that the burden is reasonable with respect to

[4] NERC Comments at 4.

[5] *Id.*

[6] *Id.* at 8 (citing Reliability Standard CIP-005-5 (Cyber Security — Electronic Security Perimeter(s)) and Reliability Standard CIP-007-6 (Cyber Security — System Security Management)).

including EACMS in the augmented reporting requirement, NERC should develop requirements based on the function of the EACMS and the nature of the attempted compromise or successful intrusion. Similarly, as discussed below, NERC should develop reporting timelines for Cyber Security Incidents that are commensurate with the adverse or attempted adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES.[7] Prioritizing incident reporting will allow responsible entities to devote resources to reporting the most significant Cyber Security Incidents faster than less significant events. With this guidance, we believe that the standard drafting team, in the first instance, is in the best position to develop the specific elements of the directed Reliability Standard requirements.

6. We have considered comments submitted by NERC and others recommending that broadened Cyber Security Incident reporting should be implemented through a request for information or data pursuant to Section 1600 of the NERC Rules of Procedure instead of through Reliability Standard requirements. However, on balance, we believe that broadened mandatory reporting pursuant to Reliability Standard requirements as opposed to a standing data request is more aligned with the seriousness and magnitude of the

[7] The NERC Glossary defines BES Cyber System 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." Glossary of Terms Used in NERC Reliability Standards (NERC Glossary). 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.

current threat environment, and more likely to improve awareness of existing and future cyber security threats and potential vulnerabilities. Four main reasons inform our decision. First, a new or modified Reliability Standard will ensure that the desired goals of our directive are met because the Commission will have the ability to review and ultimately approve the standard, as opposed to the opportunity for informal review that the Commission would have of a data request under ROP Section 1600. Second, the Commission has well-defined authority and processes under section 215(e) of the FPA to audit and enforce compliance with a Reliability Standard. Third, we do not anticipate that there will be a need to change the parameters of the Cyber Security Incident report for EACMS because the parameters that we direct below are based on five static functions of EACMS and are not technology specific, so the potential flexibility provided by a Section 1600 data request may not be significantly beneficial. Finally, collecting data through a Reliability Standard is consistent with existing practices; responsible entities are currently required to maintain the types of information that would lead to a reportable Cyber Security Incident pursuant to Reliability Standard CIP-007-6, Requirement R4.1. Nonetheless, should future events require an expedited change in data collection or should NERC desire to collect data outside the scope of the proposed Reliability Standard, NERC could then use the Section 1600 process to supplement information reported under a mandatory Reliability Standard.

7. Accordingly, pursuant to section 215(d)(5) of the FPA, we adopt the NOPR proposal and direct NERC to develop modifications to the 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, as well as modifications to specify the required information in Cyber Security Incident reports, their dissemination, and deadlines for filing reports. We direct NERC to submit the directed modifications within six-months of the effective date of this Final Rule.

I. Background

A. Section 215 and Mandatory Reliability Standards

8. Section 215 of the FPA requires a Commission-certified Electric Reliability Organization (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.[8] Pursuant to section 215 of the FPA, the Commission established a process to select and certify an ERO,[9] and subsequently certified NERC.[10]

B. Notice of Proposed Rulemaking

9. On December 21, 2017, the Commission issued a NOPR proposing to direct that NERC develop enhanced Cyber Security Incident reporting requirements. Specifically, pursuant to section 215(d)(5) of the FPA, the NOPR proposed to direct NERC to develop

[8] *Id.*

[9] *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, *order on reh'g*, Order No. 672-A, FERC Stats. & Regs. ¶ 31,212 (2006).

[10] *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).

modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS. The proposed directive was based in part on a lack of Reportable Cyber Security Incidents in 2015 and 2016, and NERC's assessment in the 2017 State of Reliability Report that "[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."[11] In addition, the NOPR stated that it agreed with the recommendation by NERC in the 2017 State of Reliability Report to "redefine reportable incidents to be more granular and include zero-consequence incidents that might be precursors to something more serious."[12]

10. In justifying the proposed inclusion of ESPs and associated EACMS within the scope of the enhanced Cyber Security Incident requirement, the NOPR stated that the purpose of an ESP is to manage electronic access to BES Cyber Systems to support the protection of the BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.[13] In addition, the NOPR explained that EACMS, which include, for example, firewalls, authentication servers, security event monitoring systems, intrusion detection systems and alerting systems, control electronic access into the ESP

[11] NOPR, 161 FERC ¶ 61,291 at P 28 (citing 2017 NERC State of Reliability Report at 4).

[12] *Id.* P 29 (citing 2017 NERC State of Reliability Report at 4).

[13] *See id.* P 33 (citing Reliability Standard CIP-005-5 (Cyber Security – Electronic Security Perimeter(s)).

and play a significant role in the protection of high and medium impact BES Cyber Systems.[14] The NOPR indicated further that, once an EACMS is compromised, an attacker could more easily enter the ESP and effectively control the BES Cyber System or Protected Cyber Asset.

11. The NOPR discussed the scope of the present Cyber Security Incident reporting requirement. The NOPR observed that Reliability Standard CIP-008-5, Requirement R1.2 currently 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. And where a Cyber Security Incident is determined to qualify as a Reportable Cyber Security Incident, the NOPR explained that responsible entities are required to notify the E-ISAC with initial notification within one hour from the determination of a Reportable Cyber Security Incident. The NOPR stated, however, that the NERC Glossary defines a Reportable Cyber Security Incident as "[a] Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity." The NOPR indicated that the definition of Reportable Cyber Security Incident, insofar as it excludes unsuccessful attempts to compromise or disrupt a responsible entity's core activities, is thus more narrow than the definition of "cybersecurity incident" in FPA section 215(a)(8), which

[14] *See id.* (citing 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).

encompasses "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."[15]

12. The NOPR stated that altering the Cyber Security Incident reporting threshold to require reporting of attempts to compromise, instead of only successful compromises, is consistent with information already logged by registered entities pursuant to current monitoring requirements in the Reliability Standards. The NOPR explained that Reliability Standard CIP-007-6, Requirement R4.1, mandates logging of detected successful login attempts, detected failed access attempts, and failed login attempts, and the Guidelines and Technical Basis for Requirement R4.1 states that events should be logged even if access attempts were blocked or otherwise unsuccessful.[16]

13. In addition to modifying the reporting threshold, the NOPR proposed to direct NERC to modify the 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, as well as the deadlines for submitting a report. Specifically, the NOPR proposed that the minimum set of attributes to be reported should include: (1) the functional impact, where possible, that the Cyber Security Incident achieved or attempted to achieve; (2) the attack

[15] 16 U.S.C. 824o(a)(8).

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

vector used to achieve or attempt to achieve the Cyber Security Incident; and (3) the level of intrusion achieved or attempted by the Cyber Security Incident. The NOPR explained that knowledge of these attributes regarding a specific Cyber Security Incident will improve awareness of cyber threats to BES reliability. The NOPR also noted that the proposed attributes are the same as attributes already used by DHS for its multi-sector reporting and summarized by DHS in an annual report.[17]

14. The NOPR also proposed to continue to require that Cyber Security Incident reports be sent to the E-ISAC instead of the Commission, but the NOPR proposed to require that such reports also be sent to ICS-CERT and that NERC file with the Commission an annual, public, and anonymized summary of such reports.

15. Finally, the NOPR sought comment on potential alternatives to modifying the mandatory reporting requirements in the NERC Reliability Standards. Specifically, the NOPR sought 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 among NERC, responsible entities and the Commission, and satisfy the goals of the proposed directive.

II. Discussion

16. Pursuant to section 215(d)(5) of the FPA, we adopt the NOPR proposal and direct NERC to develop and submit modifications to the NERC Reliability Standards to augment current mandatory reporting of Cyber Security Incidents, including incidents

[17] NOPR, 161 FERC ¶ 61,291 at P 38 (citing 2016 ICS-CERT Year in Review, https://ics-cert.us-cert.gov/Year-Review-2016).

that might facilitate subsequent efforts to harm the reliable operation of the BES. We direct NERC, subject to the discussion below, to develop and submit Reliability Standard requirements that: (1) require responsible entities to report Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS; (2) specify the required information in Cyber Security Incident reports; (3) establish deadlines for filing Cyber Security Incident reports that are commensurate with incident severity; and (4) require that Cyber Security Incident reports be sent to ICS-CERT, in addition to E-ISAC, and that NERC file with the Commission an annual, public, and anonymized summary of such reports.

17. Below, we discuss the following matters: (A) the need for broadened mandatory Cyber Security Incident reporting; (B) the threshold for a reportable Cyber Security Incident; (C) the appropriate procedural approach to augment Cyber Security Incident reporting, i.e., new or modified Reliability Standards versus a NERC data request to applicable entities; (D) the content and timing of Cyber Security Incident reports; and (E) other issues.

A. Need for Broadened Mandatory Cyber Security Incident Reporting

1. NOPR

18. In the NOPR, the Commission indicated that cyber-related event reporting is currently addressed in Reliability Standard CIP-008-5, Requirement R1.2, 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. The NOPR noted that a Cyber Security Incident is

defined in the NERC Glossary as: "A malicious act or suspicious event that: (1) compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or (2) disrupts, or was an attempt to disrupt, the operation of a BES Cyber System."

19. The Commission further explained that 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.[18] However, the NOPR observed that a Reportable Cyber Security Incident is defined more narrowly in the NERC Glossary than a Cyber Security Incident because the former requires that the incident result in the compromise or disruption of one or more reliability tasks of a functional entity. As the Commission explained, 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., reliability task) of a responsible entity that is intended to maintain BES reliability.[19] Therefore, under these definitions, unsuccessful attempts to compromise or

[18] *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.

[19] 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

disrupt a responsible entity's core activities are not subject to the current reporting requirements in Reliability Standard CIP-008-5 or elsewhere in the CIP Reliability Standards.

20. The NOPR explained that recent NERC State of Reliability Reports indicate that there were no Reportable Cyber Security Incidents in 2015 and 2016. The NOPR also highlighted NERC's conclusion that "[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."[20] The NOPR contrasted the results reported in the NERC reports with the 2016 annual summary of the Department of Energy's (DOE) Electric Disturbance Reporting Form OE-417, which contained four cybersecurity incidents reported in 2016; two suspected cyber attacks and two actual cyber attacks.[21] Moreover, the NOPR noted that ICS-CERT responded to fifty-nine cybersecurity incidents within the Energy Sector in 2016.[22]

21. Based on the comparison of information reported by NERC, DOE, and ICS-CERT, the NOPR concluded that the current reporting threshold in Reliability Standard

---

Entities, Version 5 at 7 (November 2009), http://www.nerc.com/pa/Stand/Functional%20Model%20Archive%201/Functional_Model_V5_Final_2009Dec1.pdf.

[20] 2017 NERC State of Reliability Report at 4.

[21] 2016 DOE Electric Disturbance Events (OE-417) Annual Summary Archives, https://www.oe.netl.doe.gov/OE417_annual_summary.aspx.

[22] 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.

CIP-008-5 may not reflect the true scope and scale of cyber-related threats facing responsible entities. In particular, the NOPR raised a concern that 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. The NOPR highlighted the fact that 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."[23] Agreeing with NERC's recommendation in the 2017 State of Reliability report, the NOPR proposed to direct NERC to address the apparent gap in cyber incident reporting.

2. Comments

22. NERC supports improving the reporting of Cyber Security Incidents, stating that "[b]roadening the mandatory reporting of Cyber Security Incidents would help enhance awareness of cyber security risks facing entities."[24] NERC maintains that enhanced reporting "would create a more extensive baseline understanding of the nature of cyber security threats and vulnerabilities."[25] NERC notes that broadening the scope of Cyber Security Incident reporting "is consistent with recommendations in NERC's 2017 State

[23] 2017 NERC State of Reliability Report at 4.

[24] NERC Comments at 4.

[25] *Id.* at 4.

of Reliability Report."[26] While NERC recognizes the need for enhanced Cyber Security Incident reporting, as discussed in the following sections, NERC does not support all aspects of the NOPR, including requiring enhanced cyber incident reporting through a modified Reliability Standard.

23. BPA, ITC, IRC, NYPSC, and NRG also support the NOPR proposal to direct NERC to address the gap in reporting Cyber Security Incidents. As noted by BPA, the current definition of Reportable Cyber Security Incident only addresses successful attempts to compromise or disrupt operations and, therefore, "a broader definition of a Reportable Cyber Security incident is warranted" because "information about certain attempts to compromise will likely better assist the industry in preventing successful cyber attacks."[27] BPA, ITC, and IRC raise concerns, however, regarding the risk of over-reporting. IRC states that the proposed requirement to report all attempts to compromise an ESP or associated EACMS "needs further clarification."[28] BPA states that any new reporting requirement "must ensure that the information reported is useful and does not result in under and over reporting of information."[29] NRG recommends that the term "attempt" should be clarified (i.e., as a more serious risk than a port scan) and "should be

[26] *Id.* at 4.

[27] BPA Comments at 3.

[28] IRC Comments at 1.

[29] BPA Comments at 3.

provided in technical guidance or glossary definition relating to the context of [the] existing NERC glossary term: Cyber Security Incident."[30]

24. EEI/NRECA, Trade Associations, APS, Chamber, EnergySec, Eversource, Idaho Power, and LPPC do not support the NOPR proposal to direct NERC to address the gap in reporting Cyber Security Incidents. EEI/NRECA, Trade Associations, and Chamber suggest that the Commission support existing voluntary reporting practices as opposed to mandating the reporting of Cyber Security Incidents through the CIP Reliability Standards. EEI/NRECA state that "[s]ignificant resources from responsible entities and government are engaged in […] partnerships" to share threat and vulnerability information.[31] EEI/NRECA argue that "[m]andating such sharing will overlap with these voluntary efforts and may harm the partnerships and ability of the programs to enhance cybersecurity for the electric grid."[32] In addition, EEI/NRECA state that mandating Cyber Security Incident reporting "may weaken the ability of electric companies to participate in these [voluntary reporting] programs by shifting their focus to compliance activity."[33] Eversource states that the NOPR proposal would "introduce new technical and administrative challenges that will likely impact responsible entities' ability to

[30] NRG Comments at 3.

[31] EEI/NRECA Comments at 12.

[32] *Id.* at 12.

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

participate in existing voluntary threat information sharing programs."[34] LPPC states that whatever action the Commission takes on Cyber Security Incident reporting, it "must be done with an eye towards causing as little disruption to existing information sharing programs as possible."[35]

25. Trade Associations state that while improving Cyber Security Incident reporting is an appropriate objective, "directing new or revised mandatory reliability standards is not the only tool that NERC and the Commission have for achieving that reliability objective."[36] Trade Associations contend that, in light of the constantly evolving state of cyber security, "the Commission should consider and utilize the most flexible tools to achieve its reliability goals without imposing undue burden on registered entities."[37]

26. APS states that while it "supports the Commission's objectives expressed in the NOPR," it does not agree that modifying the CIP Reliability Standards is the appropriate solution.[38] APS asserts that "the reporting requirements that already exist under Form OE-417 meet the same objectives as the Commission is attempting to satisfy by requiring additional reporting under the CIP Standards as proposed in the NOPR."[39] APS instead

[34] Eversource Comments at 5.

[35] LPPC Comments at 4.

[36] APPA, *et al.* Comments at 3-4.

[37] *Id.* at 4.

[38] APS Comments at 5.

[39] *Id.* at 7.

suggests that "the Commission … direct NERC to modify the CIP Standards to include a requirement for Responsible Entities to submit copies of its Form OE-417 to the E-ISAC and ICS-CERT."[40]

27. EnergySec states that it is "generally in agreement with the Commission's goal of increasing the frequency and detail of incident reporting," but raises concerns with the specifics of the NOPR proposal.[41] EnergySec maintains that "'compromise' as used in the definition of Reportable Cybersecurity Incident does not necessarily imply harm."[42] Therefore, EnergySec argues that "an incident should be considered a 'compromise' if an attacker has obtained the ability to disrupt, even if no disruption occurs."[43] EnergySec states further that it believes "that a clarified understanding of the current definition of Reportable Cybersecurity Incident can sufficiently address the Commission's concerns" since it "can be construed to include certain non-impactful incidents, as well as incidents affecting [ESPs] and [EACMS]."[44]

28. EnergySec also raises a concern that the NOPR proposal is too broad. EnergySec argues that determining incidents that might facilitate future cyber incidents "would be highly subjective and could easily be construed to include systems and networks that are

[40] *Id.* at 5.

[41] EnergySec Comments at 2.

[42] *Id.* at 2.

[43] *Id.* at 2.

[44] *Id.* at 3.

outside the scope of the Commission's authority."[45] EnergySec notes that most failed login or access attempts are benign in nature and "the volume of such events is orders of magnitude larger than what would be an appropriate volume for mandatory reporting."[46] EnergySec states further that while it agrees that successful attacks against ESPs and EACMS should be reported, it does not support including attempted compromise in the reporting requirements since the "[d]etermination of attempted compromise is highly subjective and it would therefore be difficult at best to clearly define within the standards a basis for such determinations."[47]

29. Eversource and Idaho Power do not support the NOPR proposal due to the anticipated increased burden that could result from increased mandatory reporting. Eversource states that "expanding the amount of required information to be reported and increasing the number of recipients of the reports will create undue administrative burdens."[48] In addition, Eversource contends that "the meaning of an attempted compromise is currently undefined and may impose significant burdens on responsible entities to identify such attempts."[49] Idaho Power states that even though "additional reporting can provide some visibility into the types of threats that entities face, additional

[45] *Id.* at 3.

[46] *Id.* at 3.

[47] *Id.* at 3-4.

[48] Eversource Comments at 1.

[49] *Id.* at 6.

administrative burdens such as reporting requirements reduce the finite resources that entities have to monitor and defend their critical infrastructure."[50]

30. LPPC asserts that the NOPR proposal "may yield a substantial quantity of unhelpful information and confusing analysis, while needlessly burdening Registered Entities."[51] LPPC states that it supports NERC's request for flexibility in addressing enhanced Cyber Security Incident reporting and concludes that "a technical conference may productively explore the nature and scope of the various programs that currently exist for information sharing regarding threats and the incremental value of any new requirements."[52] Resilient Societies states that "the modifications proposed to improve the reporting of cybersecurity incidents are unlikely to have any significant positive effect."[53] Specifically, Resilient Societies states that the proposed reporting parameters are not broad enough because "reporting of malware infection is not necessarily within thresholds set on other criteria, such as 'compromise,' 'breach,' 'impact,' or 'disruption.[54]'" Resilient Societies also suggests that the Commission convene a public technical conference.

[50] Idaho Power Comments at 2.

[51] LPPC Comments at 1.

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

[53] Resilient Societies Comments at 12.

[54] *Id.* at 10.

3. Commission Determination

31. We adopt the NOPR proposal and, pursuant to section 215(d)(5) of the FPA, direct NERC to develop and submit modifications to the Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES. Comments submitted by NERC and others support our determination that enhanced reporting of Cyber Security Incidents will address an existing gap in Cyber Security Incident reporting and will provide useful information on existing and future cyber security risks, as well as provide entities with better visibility into malicious activity prior to an event occurring. As noted in NERC's comments, "[b]roadening the mandatory reporting of Cyber Security Incidents would help enhance awareness of cyber security risks facing entities."[55] Similarly, BPA agrees with the directive to include attempted compromises in an enhanced reporting regime, stating that "information about certain attempts to compromise will likely better assist the industry in preventing successful cyber attacks."[56] Moreover, while the record reflects differing views on whether broadened Cyber Security

[55] NERC Comments at 4.

[56] BPA Comments at 3.

Incident reporting should be mandatory or voluntary, there is general agreement that improved reporting is an appropriate objective.[57]

32. Some commenters contend that the directive to require mandatory reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS is vague and requires clarification. Recognizing this concern, NERC states that "[t]he challenge is to scope any additional mandatory reporting requirements in a manner that collects meaningful data about security risks without creating an unduly burdensome reporting requirement."[58] While we address the threshold for a broadened reporting requirement issue in the next section, as a general matter, we agree with NERC that the scope of any new reporting requirement should be tailored to provide better information on cyber security threats and vulnerabilities without imposing an undue burden on responsible entities. Indeed, the NOPR proposal was not intended to be prescriptive or overly broad, but rather support NERC's efforts to enhance the reporting of Cyber Security Incidents as outlined in NERC's 2017 State of Reliability Report through the standards development process.

33. Some commenters assert that a broadened reporting requirement will overlap, duplicate or otherwise chill voluntary reporting programs, potentially diverting resources away from such programs. Other commenters, however, assert that voluntary reporting

[57] *See* NERC Comments at 4, Trade Associations Comments at 3, APS Comments at 1, BPA Comments at 3, EnergySec Comments at 1, Idaho Power Comments at 2, ITC Comments at 5, IRC Comments at 1, NRG Comments at 2-3.

[58] NERC Comments at 3.

does not adequately address the gap identified in the NOPR because voluntary reporting and mandatory reporting under currently-effective Reliability Standard CIP-008-5 have not resulted in adequate reporting of cybersecurity threats to the BES.[59] As Appelbaum notes, "[w]ithout mandatory reporting scheme a degraded threat image will result."[60]

34. Based on the record, we are not persuaded that our directive to augment current mandatory reporting requirements will adversely impact existing voluntary information sharing efforts. Instead, we agree with NERC's comment that the new "baseline understanding [resulting from broadened mandatory reporting], coupled with the additional context from voluntary reports received by the E-ISAC, [will] allow NERC and the E-ISAC to share that information broadly through the electric industry to better prepare entities to protect their critical infrastructure."[61] Moreover, we do not anticipate that the incremental burden of the directed modifications will divert significant resources from other information sharing programs since responsible entities are already required to monitor and log successful login attempts, detected failed access attempts, and failed login attempts under Reliability Standard CIP-007-6, Requirement R4.1. Nor do we anticipate that the incremental burden of complying with the directed Reliability Standards modifications would be significantly more than the burden of responding to a standing data or information request under Section 1600. We also do not believe that broadened mandatory reporting is at cross-purposes with voluntary cybersecurity-related

[59] *See id.* at 4-5.

[60] Appelbaum Comments at 7.

[61] NERC Comments at 4.

programs offered by DHS and other government agencies. We believe that voluntary programs that focus on cyber response and sharing of cyber threat information across industry are important initiatives that should be supported. However, the comments do not provide a compelling explanation why the broadening of mandatory reporting will supplant or inhibit voluntary programs.

35. While we agree with EnergySec that revisions to the current definition of Reportable Cyber Security Incident could address some aspects of our directive, a modified definition alone would not address the need to specify the required information in Cyber Security Incident reports to improve the quality of reporting and allow for ease of comparison, or establish deadlines for submitting a report to facilitate timely information sharing. Therefore, while we believe that a modified definition of Reportable Cyber Security Incident could address part of the Commission's concerns, additional modifications would be necessary to meet the full scope of our directive.

36. In addition, we do not agree with Resilient Societies that the detection of malware infecting a responsible entity's ESP or associated EACMS would fall outside the new reporting requirement. While Resilient Societies asserts that a malware infection would not meet the threshold of a compromise, breach, impact, or disruption, we believe that it would fall within the parameters of an attempted compromise. As discussed in the next section, however, we believe that it is appropriate for NERC to address the reporting threshold through the standards development process in order to weigh the diverse technical opinions on how to identify the appropriate assets and the level of attempted compromise that warrants reporting. Accordingly, we are not persuaded to convene a

technical conference. Rather, persons interested in the development of appropriate detailed parameters of the augmented reporting requirements should participate in the NERC standards development process.

37. In sum, we conclude that the record supports our determination that directing NERC to develop and submit modifications to the Reliability Standards to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's ESP, as well as associated EACMS, is appropriate to carry out FPA section 215. Therefore, pursuant to FPA section 215(d)(5), we direct NERC to develop and submit modifications to the 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. As noted above, we direct NERC to submit the directed modifications within six-months of the effective date of this Final Rule.

B. Threshold for a Reportable Cyber Security Incident

1. NOPR

38. The NOPR proposed to direct NERC to modify the 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. The NOPR explained that reporting attempts to compromise, instead of only successful compromises, is consistent with current monitoring requirements in Reliability Standard CIP-007-6, Requirement R4.1, which mandates logging of detected successful login attempts,

detected failed access attempts and failed login attempts.[62] In addition, the NOPR identified other reporting regimes that include attempts within the general definition of a "cyber incident." Specifically, DHS defines a "cyber incident" as "attempts (either failed or successful) to gain unauthorized access to a system or its data…."[63] The E-ISAC defines a "cyber incident" as including unauthorized access through the electronic perimeter as well as "a detected effort … without obvious success."[64] And ICS-CERT defines a "cyber incident" as an "occurrence that actually or potentially results in adverse consequences…."[65]

39. As noted above, 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 compromise that could lead to misoperation or instability in the BES. The NOPR explained that since an ESP is intended to protect BES Cyber Systems, it is reasonable to establish the compromise of, or attempt to compromise, an ESP as the minimum reporting threshold.

---

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

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

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

[65] *See* ICS-CERT Published "Common Cyber Security Language" document: https://ics-cert.us-cert.gov/sites/default/files/documents/Common%20Cyber%20Language_S508C.pdf.

40. In addition, the NOPR identified an ESP's associated EACMS as another threshold for a Reportable Cyber Security Incident. As explained in the NOPR, 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.

41. While the Commission proposed to include EACMS within the scope of the proposed directive, the Commission also sought comment on the possibility of excluding EACMS from the scope of the proposed directive.

2. Comments

42. NERC supports the NOPR proposal to limit the scope of Cyber Security Incident reporting to incidents that compromise or attempt to compromise a responsible entity's ESP or associated EACMS. NERC explains that any new reporting requirements "need to be scoped in a manner that provides for meaningful reporting of cyber security risks but does not unduly burden entities."[66] Specifically, NERC states:

> Because the ESP protects some of the most important Cyber Assets and the EACMS control or monitor access to those Cyber Assets, NERC agrees that reporting on attempts to compromise these security measures would provide valuable data while also imposing a reasonable burden on entities given the limited traffic they should experience.[67]

[66] NERC Comments at 6.

[67] *Id.* at 7.

NERC notes that some EACMS devices "may provide important early indicators of future compromise" and, therefore, NERC states that it "supports including EACMS in the reporting threshold in addition to the ESP and notes that logging attempts to compromise the ESP and some EACMS devices does not impose an unreasonable burden on entities."[68]

43. While NERC supports adopting the compromise or attempt to compromise a responsible entity's ESP or an EACMS associated with an ESP as a threshold for Cyber Security Incident reporting, NERC explains that "there is still a need to refine the scope of the proposed directive to ensure that it would provide meaningful data without overburdening entities."[69] Specifically, NERC states that there is a need to "outline the parameters of an 'attempt to compromise' in order to issue a precise data request."[70] In particular, NERC states that it "would consider the common understanding of adverse activities that are early indicators of compromise, such as campaigns against industrial control systems, to help refine the parameters."[71] In addition, NERC notes that EACMS, as defined in the NERC Glossary, include a wide variety of devices that perform control and monitoring functions. NERC states further that it "needs to consider whether to define the reporting threshold to differentiate between the various types of EACMS for

[68] *Id.* at 8.

[69] *Id.* at 9.

[70] *Id.* at 9.

[71] *Id.* at 9.

reporting purposes."[72] Therefore, NERC requests that the Commission provide flexibility in refining the threshold for Cyber Security Incident reporting.

44. Trade Associations, APS, BPA, EnergySec, Resilient Societies, IRC, ITC, and NYPSC generally support the reporting threshold proposed in the NOPR, but caution that any new or modified requirements should be properly scoped. Trade Associations state that the NOPR proposal "is potentially overbroad and could result in unduly burdensome reporting requirements that *reduce* awareness of significant cyber threats."[73] Trade Associations also contend that a new or revised Reliability Standard "should not include the proposed generic threshold of reporting *any* incidents that compromise or attempt to compromise an ESP or EACMS."[74] Instead, Trade Associations recommend that the Commission "give NERC sufficient flexibility to define appropriate reporting thresholds for attempted compromises of an ESP or EACMS."[75]

45. APS asserts that, given the differences among EACMS, it does not support the inclusion of all EACMS or the exclusion of all EACMS from an enhanced reporting requirement. APS states that while it "concurs that the incidents impacting the ESP should certainly be in scope of reporting, it is concerned that the exclusion of EACMS (which includes [Electronic Access Points (EAP)]) results in a likely compromise

[72] *Id.* at 9.

[73] APPA, *et al*. Comments at 5 (emphasis in original).

[74] *Id.* (emphasis in original).

[75] *Id.* at 5.

scenario going unreported."[76] Specifically, APS notes that "a user's credentials to an Intermediate System, which includes/can be classified as an EAP(s) and/or EACMS, could be compromised."[77] APS contends that such a compromise would not implicate the ESP, but could impact or attempt to impact a BES Cyber Asset or System. APS states, however, that "there are numerous EACMS for which a compromise scenario would not be critical or allow potential access to an ESP."[78] Therefore, APS maintains that an evaluation of the functions of various EACMS is needed before they can be included in any reporting requirement.

46. BPA states that a broader definition of a Reportable Cyber Security Incident is necessary since the current definition only addresses actual compromises. BPA avers that "information about certain attempts to compromise will likely better assist the industry in preventing successful cyber attacks."[79] BPA states that the current definition of a Cyber Security Incident is a good starting point for a revision since it includes attempts to compromise or disrupt. BPA cautions, however, that the current definition of Cyber Security Incident "may be too broad and result in overreporting of information."[80]

[76] APS Comments at 9.

[77] *Id.*

[78] *Id.*

[79] BPA Comments at 3.

[80] *Id.* at 3.

47. EnergySec states that it "generally agree[s] that successful attacks against ESPs and EACMS should be within the scope of reporting; [but] disagree[s] with the proposal to include attempted compromise in the reporting requirements."[81] In addition, EnergySec suggests that monitoring-only systems be excluded from any reporting requirement, stating that "[a]lthough compromise of monitoring systems could assist an attack, such a compromise would not directly permit access."[82] Resilient Societies states that "[e]xcluding [EACMS] from the Commission directive could exempt reporting of attempted compromises."[83] IRC states that "adding EACMS to the requirement for mandatory reporting would be beneficial, not only because of their role as a boundary point, but also because EACMS perform other roles that support the BES Cyber Systems."[84] IRC cautions, however, that "[w]ithout providing further definitions or criteria, the NOPR's proposal to require reporting of all 'attempts to compromise' the ESP or EACMS is unclear and potentially unachievable."[85]

48. While ITC generally supports the NOPR proposal, ITC "requests that the Commission refrain from including unsuccessful attempts to compromise an ESP-

[81] EnergySec Comments at 3-4.

[82] *Id.* at 4.

[83] Resilient Societies Comments at 14.

[84] IRC Comments at 5.

[85] *Id.* at 3-4.

associated EACMS in the revised definition of a Cyber Security Incident."[86] ITC notes that responsible entity systems with publicly-visible IP addresses "sustain a regular stream of denial of service attempts, phishing emails, attempted firewall breaches, untargeted and targeted malware, and other common cybersecurity threats for which countermeasures are well-established and which pose a miniscule chance of success."[87] ITC states that including "attempted compromises of ESP-associated EACMS would appear to require reporting for a sizeable number of these common events."[88] Therefore, ITC states that while it "supports expanding the definition of Reportable Cyber Incidents to include incidents that compromise, or attempt to compromise, a responsible entity's ESP, ITC would urge the Commission to direct NERC to include only actual breaches of a responsible entity's ESP-associated EACMS, and not attempted-but-unsuccessful compromises."[89] NYPSC notes that "[f]ailed cyber attacks occur on a continuous basis, all the time…" and, therefore, "[a] reporting requirement of every attempted security attack may be overly burdensome for reporting entities."[90] NYPSC "suggests FERC

[86] ITC Comments at 5.

[87] *Id.* at 5.

[88] *Id.* at 5.

[89] *Id.* at 5.

[90] NYPSC Comments at 5-6.

consider developing clear criteria of the required reporting based on its review of the comments and recommendations from reporting entities."[91]

49. Idaho Power states that "additional reporting requirements do not increase cyber security."[92] Idaho Power contends that "additional administrative burdens such as reporting requirements reduce the finite resources that entities have to monitor and defend their critical infrastructure."[93] In addition, Idaho Power states that EACMS "should be excluded from any additional requirements and only BES Cyber Systems and associated devices should be included in any further reporting requirements."[94]

50. Other commenters support expanding the enhanced reporting requirement beyond what was proposed in the NOPR. NRG supports the NOPR proposal to direct NERC to develop modifications to the CIP Reliability Standards to improve the reporting of Cyber Security Incidents. NRG also supports including EACMS as a threshold for reporting. In addition, NRG "recommends that the scope of the NOPR avoid limiting the requirement to High and Medium Impact BES Cyber Systems."[95] Specifically, NRG notes that the NOPR proposal "would limit the requirement to High and Medium Impact BES Cyber Systems as ESPs and EACMS are not required establishments at Low Impact BES Cyber

[91] *Id.* at 6.

[92] Idaho Power Comments at 2.

[93] *Id.*

[94] *Id.*

[95] NRG Comments at 5.

Systems."[96] Therefore, NRG states that "any modification to the referenced CIP Reliability Standards should be applicable to all BES Cyber Systems with External Routable Communications."[97]

51. Appelbaum supports the NOPR proposal to include the attempted or actual compromise of an ESP or EACMS in the mandatory reporting requirement. However, Appelbaum "propose[s] the Commission consider adding Physical Security Perimeters and Physical Access Control Systems (PACS) as well."[98] Simon supports the NOPR proposal, but encourages the Commission to broaden the directive to include low impact BES Cyber Systems. Specifically, Simon states that "[o]mission of mandatory reporting for the disruption, or an attempt to disrupt, the operation of electronic access controls for BES assets with low impact BES Cyber Systems leaves a large blind spot in the Commission's effort to learn of efforts to harm the reliable operation of the bulk electric system."[99] Isologic does not support limiting Cyber Security Incident reporting to situations involving an entity's ESP or associated EACMS. Isologic states that "there are few CIP standards for 'secure perimeters' and for the mass of BES Low Impact Facilities, (substations), security is at the fence line, not in ESPs."[100]

[96] *Id.* at 2.

[97] *Id.*

[98] Appelbaum Comments at 7.

[99] Simon Comments at 4.

[100] Isologic Comments at 7.

3. Commission Determination

52. The record in this proceeding supports establishing the compromise or attempted compromise of an ESP as the appropriate threshold for a Reportable Cyber Security incident. In addition, with exceptions, the comments support including EACMS associated with an ESP as part of the reporting threshold. As NERC notes, an "ESP protects some of the most important Cyber Assets and the EACMS control or monitor access to those Cyber Assets."[101] While we believe that ESPs and EACMS should be within the scope of a broadened reporting requirement, the comments, correctly in our view, point to the need to establish an appropriate scope for reporting. As NERC states, "there is still a need to refine the scope of the proposed directive to ensure that it would provide meaningful data without overburdening entities."[102] This concern is reflected in a number of comments, pointing to the need to identify the appropriate assets to monitor (for example, only EACMS associated with an ESP) and to clearly define an "attempt to compromise."[103]

53. The comments generally support the view that NERC should have the flexibility to establish an appropriate reporting threshold. We recognize the need for a certain level of flexibility and believe that it is appropriate for NERC to address the specific reporting threshold through the standards development process. However, as discussed further

[101] NERC Comments at 7.

[102] *Id.* at 9.

[103] *See* NERC Comments at 9, APPA, *et al*. Comments at 5, APS Comments at 9, BPA Comments at 3, EnergySec Comments at 3, IRC Comments at 3-4, ITC Comments at 5, NYPSC Comments at 6.

below, we provide guidance on certain aspects of how NERC should identify EACMS for reporting purposes and what types of attempted compromise must be reported.

54. With regard to identifying EACMS for reporting purposes, NERC's reporting threshold should encompass the functions that various electronic access control and monitoring technologies provide. Those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting.[104] Reporting a malicious act or suspicious event that has compromised, or attempted to compromise, a responsible entity's EACMS that perform any of these five functions would meet the intended scope of the directive by improving awareness of existing and future cyber security threats and potential vulnerabilities. Since responsible entities are already required to monitor and log system activity under Reliability Standard CIP-007-6, the incremental burden of reporting of the compromise or attempted compromise of an EACMS that performs the identified functions should be limited, especially when compared to the benefit of the enhanced situational awareness that such reporting will provide.

55. With regard to the definition of "attempted compromise" for reporting purposes, we consider attempted compromise to include an unauthorized access attempt or other

[104] *See* NERC Glossary of Terms definition of EACMS. *See also* Reliability Standard CIP-006-6, Requirement R1.5 (Physical Security Plan) at 10 ("[i]ssue an alarm or alert in response to detected unauthorized access" to certain High and Medium Impact BES Cyber Systems and associated EACMS); Reliability Standard CIP-007-6, Requirement R4.2 (Security Event Monitoring) at 16; and Reliability Standard CIP-007-6, Requirement R5.7 (System Access Control) at 25.

confirmed suspicious activity. ITC raises a concern that including unsuccessful attempts to compromise an EACMS associated with an ESP would require reporting a significant number of events. We note, however, that limiting the reporting threshold to only EACMS that are associated with an ESP should limit the reporting burden since these assets should be located apart from the responsible entity's broader business IT networks. Moreover, as discussed in the next section, we also believe that a flexible reporting timeline that reflects the severity of a Cyber Security Incident could also help address the potential burden of reporting attempted compromises.

56. With regard to BPA's suggestion that a revised definition of Reportable Cyber Security Incident is necessary, as discussed above, revisions to the current definition of Reportable Cyber Security Incident could address certain aspects of the NOPR proposal, although a modified definition alone would not address the need to specify the required information in cyber security incident reports to improve the quality of reporting and allow for ease of comparison, or establish deadlines for submitting a report to facilitate timely information sharing. Therefore, although we believe that a modified definition of Reportable Cyber Security Incident could address part of the Commission's concerns, additional modifications to the Reliability Standards would be necessary to meet the security objective of the directives discussed herein.

57. A number of commenters request that we expand the directive to include a broader scope of assets, including low impact BES Cyber Systems. However, we decline to expand the scope of Cyber Security Incident reporting beyond the ESP and associated EACMS at this time. The focus on ESPs and associated EACMS is intended to provide

threat information on BES Cyber Systems that have the greatest impact on BES reliability while imposing a reasonable reporting burden on responsible entities. Nevertheless, the Commission could revisit this issue if there is demonstrated need for expanded Cyber Security Incident reporting.

58. Therefore, we adopt the NOPR proposal and conclude that the compromise, or attempt to compromise, a responsible entity's ESP or associated EACMS is a reasonable threshold for augmented Cyber Security Incident reporting.

C. Appropriate Procedural Approach to Augment Cyber Security Incident Reporting

1. NOPR

59. The NOPR proposed to direct NERC to modify the CIP Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, while also seeking 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.

2. Comments

60. While NERC supports broadened mandatory Cyber Security Incident reporting, NERC does not support the NOPR proposal to direct a modification to the Reliability Standards. Instead, NERC requests flexibility to determine the appropriate reporting procedure. Specifically, NERC proposes to "use the [Rules of Procedure] Section 1600 process for gathering data used for system performance."[105] NERC maintains that it has

[105] NERC Comments at 10.

"successfully shifted to using Section 1600 for other data collection efforts, such as the collection of reports on Protection System Misoperation."[106] NERC explains further that the Section 1600 process would be used to "supplement the existing voluntary reporting of cyber security threats to E-ISAC."[107]

61. NERC states that the Section 1600 process "provides many of the same benefits as Reliability Standards," such as stakeholder and Commission staff input.[108] NERC also states that, similar to Reliability Standards, compliance with Section 1600 is mandatory. NERC explains that if a responsible entity does not respond to a Section 1600 data request, "NERC has the authority under the [Rules of Procedure] to take such action as NERC deems appropriate to address a situation where a Rule of Procedure cannot practically be complied with or has been violated."[109] NERC explains that the Section 1600 data request process provides the flexibility to revise or update the data request, if necessary, as well as "the flexibility to determine the appropriate timeline for submitting the data."[110] NERC states that while it may continue to use the Reliability Standards for data collection for evidence of compliance or to facilitate sharing of information between entities for BES operations, it "has found the [Rules of Procedure] Section 1600 process

[106] *Id.*

[107] *Id.*

[108] *Id.*

[109] *Id.* at 11.

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

to be effective for data collection to assess system performance."[111] NERC cites a standing Section 1600 data request for entities to submit quarterly data on Protection System Misoperations as an example.

62. LPPC supports the use of the Section 1600 process to facilitate enhanced Cyber Security Incident reporting. LPPC states that it "supports a more flexible approach to collection of actionable information through the data request process outlined in NERC ROP Section 1600."[112] LPPC asserts that the data request approach offers flexibility that the standards development process does not. Specifically, LPPC states that "compliance with a NERC data request is mandatory for applicable entities, while the data request procedures specified under [Rules of Procedure] Section 1600 also provide a more efficient process to update or revise a data request as needed to respond to rapidly-changing security threats."[113] Finally, LPPC opines that "it seems appropriate to remove the data collection process from the enforcement process associated with mandatory Reliability Standards."[114]

63. APS, BPA, Resilient Societies, IRC, and NRG oppose the use of the Section 1600 process to facilitate enhanced Cyber Security Incident reporting. APS asserts that a request for data pursuant to Section 1600 would not effectively address the reporting gap

[111] *Id.* at 12.

[112] LPPC Comments at 6-7.

[113] *Id.* at 7.

[114] *Id.*

and current lack of awareness of cyber-related incidents. Specifically, APS argues that a data request would create an independent, redundant reporting obligation to NERC or a regional entity and would subject the provisions of reported information to the confidentiality and data sharing processes set forth in Rules of Procedure Section 1500, unnecessarily delaying sharing and distribution of information.[115] APS states further that the Section 1600 process "adds significant additional administrative burden for all involved entities, which is inefficient and unnecessary and presents a potential obstacle to the very sharing and distribution that is a critical part of the Commission's objectives set forth in the NOPR."[116]

64. BPA comments that a data request is not an effective means of obtaining information about cyber security incidents. BPA explains that Section 1600 data requests "are one time requests for existing data, and […] not the appropriate vehicle for ensuring ongoing reporting necessary to make data about Cyber Security Incidents effective."[117] Resilient Societies states that "[e]xamination of NERC Rules of Procedure Section 1600 shows the intent of [the] rule is to facilitate one-time requests for data."[118] Therefore, Resilient Societies asserts that the Section 1600 reporting procedures "would be a poor fit for a standing order for data on cybersecurity incidents that occur continually."[119] NRG

[115] APS Comments at 16.

[116] *Id.* at 16-17.

[117] BPA Comments at 4.

[118] Resilient Societies Comments at 15.

[119] *Id.*

opposes the use of the Section 1600 data request process asserting that a request for data or information would neither address the current lack of awareness of cyber-related incidents, nor satisfy the goals of the proposed directive.

65. APS, as discussed above, suggests adopting the DOE Electric Disturbance Events, Form OE-417 as the primary reporting tool for Cyber Security Events. EnergySec, for its part, suggests that the Commission could direct NERC to require entities to develop and implement an information sharing plan.[120] According to EnergySec, such an approach should provide broad discretion to entities and ensure that compliance oversight efforts cannot result in second-guessing of decisions regarding which information to share, when, or with whom. IRC suggests, alternatively, that the Commission allow entities to comply with the reporting requirements by participating in the Cyber Risk Information Sharing program. IRC explains that the program allows entities to automatically report information to E-ISAC for analysis against classified information. IRC states that responsible entities that "automatically report indicators of compromise through these systems will share information at machine speed, and this should be considered superior to manual reporting, which requires much slower decision-making."[121]

3. Commission Determination

66. As discussed above, we adopt the NOPR proposal and direct NERC to develop modifications to the NERC Reliability Standards to improve mandatory reporting of

[120] EnergySec Comments at 6.

[121] IRC Comments at 7.

Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the BES. We have considered the arguments raised in the comments for using Reliability Standards, Section 1600 information and data requests, and other vehicles to implement augmented Cyber Security Incident reporting. On balance, we conclude that broadened mandatory reporting pursuant to Reliability Standard requirements is more aligned with the seriousness and magnitude of the current threat environment and the more effective approach to improve awareness of existing and future cyber security threats and potential vulnerabilities.

67. First, the development of a Reliability Standard provides the Commission with an opportunity to review and ultimately approve a new or modified Reliability Standard, ensuring that the desired goals of the directive are met. Moreover, the Reliability Standards development process allows for the collaboration of industry experts in developing a draft standard and also gives interested entities broader opportunity to participate and comment on any proposal that is developed. In contrast, NERC's process for developing a Section 1600 data request provides for less stakeholder input and only informal review of a draft data request by Commission staff. Thus, in this circumstance, the standards development process is preferable for the development of augmented cyber incident reporting requirements that satisfy the scope of the Commission's directive.

68. Second, the development of a Reliability Standard provides better assurance of accurate, complete, and verifiable reporting of cyber security incidents. The Commission has well-defined authority and processes under section 215(e) of the FPA to audit and enforce compliance with a Reliability Standard. While NERC notes that a responsible

entity must respond to a NERC Section 1600 data request, NERC cannot impose sanctions on registered entities who fail to respond to such data requests. Rather, a failure to comply would be a violation of the Commission's regulations,[122] requiring a referral to the Commission for action. Such a process would be a departure from the clearly defined processes used to enforce compliance with the Reliability Standards. Moreover, it is unclear how NERC would even learn of such a failure since, unlike mandatory Reliability Standards, compliance with Section 1600 data requests are not subject to regular audit. Accordingly, given the importance of accurate, complete, and verifiable cyber security incident reporting, we find that the more robust and well-established compliance and enforcement processes associated with mandatory Reliability Standards are desirable in this instance.

69. Third, we are not persuaded by NERC's assertion that a Section 1600 data request is preferable in this instance because it allows for flexibility and faster modification should a need arise for future revisions to the collection of cyber incident reporting data. We do not anticipate that there would be a need to change the parameters of the event report, given that the anticipated reporting requirements should not be technology-specific, but rather, broad enough to capture basic data even as the nature of cyber security incidents evolve. Specifically, the NOPR proposed that the minimum set of

[122] 18 CFR 39.2(b) (2017) ("All entities subject to the Commission's reliability jurisdiction…shall comply with applicable Reliability Standards, the Commission's regulations, and applicable Electric Reliability Organization and Regional Entity Rules made effective under this part.")

attributes to be reported should include: (1) the functional impact, where possible to determine, 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. Since these attributes are general in nature and not technology specific, they would not need to be refined as the underlying cyber threats evolve, nor would they need to be refined quickly.

70. In a similar vein, the assets (i.e., EACMS) subject to the enhanced reporting requirements should be identified based on function, as opposed to a specific technology that could require a modification in the reporting requirements should the underlying technology change. As discussed above, those functions must include, at a minimum: (1) authentication; (2) monitoring and logging; (3) access control; (4) interactive remote access; and (5) alerting. Finally, since the level of attempted compromise that warrants reporting should reflect unauthorized access attempts and other confirmed suspicious activity, we do not anticipate that a modification would be required in the future. Nevertheless, should the situation demand a more timely change in data collection or should NERC desire to collect additional information that is outside the scope of the proposed Reliability Standard, NERC could use the Section 1600 data request process to supplement information reported under a mandatory Reliability Standard.

71. Finally, requiring a data collection in a Reliability Standard is consistent with existing practices since responsible entities are currently required to maintain the types of

information that would lead to a reportable Cyber Security Incident pursuant to Reliability Standard CIP-007-6, Requirement R4.1.

72. While we recognize that NERC could likely develop a Section 1600 data request more quickly than a mandatory Reliability Standard, given the potential complexity of considering reporting requirements for the various EACMS, we believe that the technical depth of a standard development process is more appropriate for this case. Although NERC states that it has successfully used ROP Section 1600 to collect data on system performance, in this circumstance the information being reported relates to threats and potential compromises that may require immediate or near-term action as opposed to retrospective reporting on Misoperations, as Section 1600 has been used.

73. We also do not support adopting the DOE Form OE-417 as the primary reporting tool for reporting Cyber Security Incidents, as suggested by some commenters. The reporting criteria in our directive are distinguishable and more aligned with a risk management approach than the information requested in the DOE Form OE-417. Specifically, the DOE Form OE-417 has twelve generic criteria for filing a report to the DOE, of which only two reflect the criteria outlined in the NOPR proposal, which are discussed in the following section. The DOE Form OE-417 does not address factors such as attack vector, functional impact and level of intrusion. In addition, the definition of a "Cyber Event" in the DOE Form OE-417 filing instructions does not align with the definition of Cyber Security Incident in the NERC Glossary of Terms, let alone a

Reportable Cyber Security Incident.[123] Nor does the DOE Form OE-417 require reporting to E-ISAC or ICS-CERT as our directive requires.

74. In sum, we conclude that 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 BES, is the appropriate approach to improve Cyber Security Incident reporting.

D. Content and Timing of a Cyber Security Incident Report

1. NOPR

75. The NOPR proposed to direct that NERC modify the CIP Reliability Standards to specify the required content in a Cyber Security Incident report. Specifically, the NOPR proposed that the minimum set of attributes to be reported should 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 attempt 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. The NOPR noted that the proposed attributes are the same as attributes already used by DHS for its multi-sector reporting and summarized by DHS in an annual report. The NOPR stated that specifying the required content should improve the quality of reporting by ensuring that basic information is provided; and

[123] *See* Department of Energy Electric Emergency Incident and Disturbance Report – Form OE 417. Form OE-417 defines a Cyber Event as a disruption on the electrical system and/or communication system(s) caused by unauthorized access to computer software and communications systems or networks including hardware, software, and data. https://www.oe.netl.doe.gov/oe417.aspx

allowing for ease of comparison across reports by ensuring that each report includes specified fields of information. The NOPR sought comment on the proposed attributes and, more generally, the appropriate content for Cyber Security Incident reporting to improve awareness of existing and future cyber security threats and potential vulnerabilities.

76. In addition, the NOPR proposed to direct NERC to establish requirements outlining deadlines for filing a report once a compromise or disruption to reliable BES operation, or an attempted compromise or disruption, is identified by a responsible entity. The NOPR stated that the reporting timeline should reflect the actual or potential threat to reliability, with more serious incidents reported in a more timely fashion. The NOPR explained that a reporting timeline that takes into consideration the severity of a Cyber Security Incident should minimize potential burdens on responsible entities.

77. The NOPR also proposed that the reports submitted under the enhanced mandatory reporting requirements would be provided to E-ISAC, similar to the current reporting scheme under Reliability Standard CIP-008-5, as well as ICS-CERT or any successor organization. While the NOPR stated that the detailed incident report would not be submitted to the Commission, the NOPR proposed to direct NERC to file publicly an annual report reflecting the Cyber Security Incidents reported to NERC during the previous year. Specifically, the NOPR proposed to direct NERC to file annually an

anonymized report providing an aggregated summary of the reported information, similar to the ICS-CERT annual report.[124]

2. Comments

78. NERC supports the minimum set of reporting attributes proposed in the NOPR, stating that "this level of detail regarding each reported Cyber Security Incident will not only help NERC understand the specific threat but also help NERC understand trends in threats over time."[125] NERC also does not oppose either filing an annual, anonymized summary of the reports with the Commission, or submitting the reports of U.S.-based entities to the ICS-CERT in addition to E-ISAC. Finally, while NERC supports the concept of imposing a deadline for entities to submit full reports of Cyber Security Incidents, NERC requests flexibility to determine the appropriate timeframe. Specifically, NERC states that it "will determine an appropriate deadline for reports so that NERC can use the data for awareness and early indicators of potential compromise but also consider whether reporting for historical analysis can provide insight to the trends and effectiveness of industry's security controls."[126]

79. ITC, IRC, and NRG support the minimum set of reporting attributes proposed in the NOPR. ITC states that the NOPR proposal reflects "a reasonable set of baseline

[124] NOPR, 161 FERC ¶ 61,291 at 42.

[125] NERC Comments at 14.

[126] *Id.*

requirements for reporting."[127] While ITC raises a concern that the collective information in a report could potentially lead to the identification of the reporting entity, ITC states that it "will work within the NERC stakeholder and standards development process to ensure that the Standards submitted in response to the Commission's final rule are structured to preserve anonymity to the maximum extent practicable."[128] IRC asserts that "it will be beneficial for responsible entities to report indicators of compromise that are detected in potential cyberattacks against their systems in standard form."[129] NRG recommends that mandatory reporting include: "content Date, Time, Duration of Incident, Origination of the attack, threat vector, targeted system (or OS), vulnerability exploited, [and] method used to stop/prevent the attack."[130]

80. Appelbaum, APS, EnergySec, Resilient Societies, and Idaho Power raise concerns with the minimum set of reporting attributes proposed in the NOPR. According to Appelbaum, a count by category of asset, attack vector, and impact is sufficient for the mandatory reporting. APS contends that "because each entity's network topology, architecture, applications, and other characteristics are different, any requirement to

[127] ITC Comments at 6.

[128] *Id.*

[129] IRC Comments at 7.

[130] NRG Comments at 5.

provide the functional impact and level of intrusion as part of reporting is of very low value and should not be included as mandatory attributes of reporting."[131]

81. APS, however, "agrees that information regarding attack vectors could be more relevant, actionable information to be shared."[132] EnergySec expresses concern that including the proposed set of reporting attributes as a requirement could be construed to require significant forensic and analysis efforts. Resilient Societies suggests that the Commission leverage prior work done by the federal government as opposed to establishing new report content. Specifically, Resilient Societies suggests that the Commission adopt the US-CERT "Federal Incident Notification Guidelines." Idaho Power states that a "description of the event and the system(s) affected along with a fact pattern describing the situation and known information at the time the report is submitted should be sufficient."[133]

82. With regard to the timing of reports, ITC questions whether an initial report of a Cyber Security Incident would have to be submitted to ICS-CERT as well as E-ISAC. ITC opines that "the existing one-hour reporting requirement poses a significant compliance challenge, and that requiring that the initial report also be provided to ICS-CERT would be unworkable under that timeframe."[134] IRC states that "[t]he timeframe

---

[131] APS Comments at 11-12.

[132] *Id.* at 12.

[133] Idaho Power Comments at 3.

[134] ITC Comments at 7.

for completing a full report depends on the scale and scope of the investigation [and] FERC should consider requiring that reports be updated at a certain frequency until the full report is complete."[135] IRC recommends a 90-day update requirement until a report is finalized. NRG recommends that Cyber Security Incident reports should be submitted after existing industry processes have been followed relating to Incident Reporting and Response Plans. In addition, NRG recommends that the Commission consider directing NERC to file a quarterly report in addition to the annual report.

83. APS recommends aligning the timing of any mandatory reporting obligations with the timing dictated in Form OE-417. APS contends that reporting events that "could, but didn't, cause harm to the BES and/or facilitate subsequent efforts to harm … should be far enough removed from the incident to not divert resources from incident response and to ensure that enough details are known about the incident to provide an accurate, thorough report.[136]

84. EnergySec agrees that clear timelines should be included in any new mandatory Cyber Security Incident requirements. EnergySec further comments that the timelines should factor in the severity of the incident and the level of effort required to complete an investigation. Resilient Societies offers that "[i]n an ideal world, reporting of cybersecurity incidents would take place at machine speed" and suggests that the

[135] IRC Comments at 8.

[136] APS Comments at 13.

Commission "allow and preferably require automated reporting, at least for an initial report."[137] Idaho Power states that, should the Commission require timelines for reporting, it should ensure that an entity has adequate time to analyze each event before the reporting deadline.

85. Lasky supports entities being required to report Cyber Security Incidents to both E-ISAC and ICS-CERT, and states that "it would be prudent to report all incidents to the United States Cyber Emergency Response Team (US-CERT)" as well.[138]

3. Commission Determination

86. As discussed below, we adopt the NOPR proposal on minimum reporting attributes and timing, in response to the commenters' concerns, but we also leave discretion to NERC to develop the reporting timelines in the standards development process by considering several factors so that the timelines provide for notice based upon the severity of the event and the risk to BES reliability, with updates to follow initial reports.

87. The comments generally support the proposed minimum set of reporting attributes. For example, NERC supports the proposed content for a Cyber Security Incident report, while requesting flexibility to determine the appropriate reporting timeframe. As noted by ITC, the NOPR proposal reflects "a reasonable set of baseline

[137] Resilient Societies Comments at 15.

[138] Lasky Comments at 1.

requirements for reporting."[139] Certain comments do raise concerns with the proposed reporting attributes, especially in the case of attempts versus actual compromises.

88. In our view, a new or revised Cyber Security Incident report should include, at a minimum, the information outlined in the NOPR proposal, where available. Specifically, the minimum set of attributes to be reported should 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 or as a result of the Cyber Security Incident. In addition, we agree that any reporting requirement should not take away from efforts to mitigate a potential compromise.

89. With regard to timing, we conclude that NERC should establish reporting timelines for when the responsible entity must submit Cyber Security Incident reports to the E-ISAC and ICS-CERT based on a risk impact assessment and incident prioritization approach to incident reporting.[140] This approach would establish reporting timelines that are commensurate with the adverse impact to the BES that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Higher risk incidents, such as detecting malware within the ESP and associated EACMS or an

[139] ITC Comments at 6.

[140] Similar to the Cyber Incident Severity Schema in DHS's National Cyber Incident Response Plan, Annex D (Reporting Incidents to the Federal Government) at 41 (2016), https://www.us-cert.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf.

incident that disrupted one or more reliability tasks, could trigger the report to be submitted to the E-ISAC and ICS-CERT within a more urgent timeframe, such as within one hour, similar to the current reporting deadline in Reliability Standard CIP-008-5.[141] For lower risk incidents, such as the detection of attempts at unauthorized access to the responsible entity's ESP or associated EACMS, an initial reporting timeframe between eight and twenty-four hours would provide an early indication of potential cyber attacks.[142] For situations where a responsible entity identifies other suspicious activity associated with an ESP or associated EACMS, a monthly report could, as NERC states, assist in the analysis of trends in activity over time.[143]

90. With regard to the appropriate recipients for Cyber Security Incident reports, we determine that the reports should be provided to E-ISAC, similar to the current reporting

[141] An example of incident categories is the Chairman of the Joint Chiefs of Staff Manual, Cyber Incident Handling Program, Enclosure B, Appendix A to Enclosure B (Cyber Incident and Reportable Cyber Event Categorization) (2012), http://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897.

[142] *See* Department of Energy Electric Emergency Incident and Disturbance Report, Form OE-417 (six-hour reporting deadline for cyber events that could potentially impact electric power system reliability) found at: https://www.oe.netl.doe.gov/docs/OE417_Form_05312021.pdf; Nuclear Regulatory Commission Regulatory Guide 5.71 (four-hour reporting deadline for cyber events that could have caused an adverse impact) found at: https://www.nrc.gov/docs/ML0903/ML090340159.pdf; *see also* Reliability Standard EOP-004-3 (Event Reporting), Requirement R2 (requiring a report within twenty-four hours for an events that impact or may impact BES reliability).

[143] *See* NERC Comments at 14.

scheme under Reliability Standard CIP-008-5, as well as ICS-CERT or its successor.[144] Reporting directly to E-ISAC and ICS-CERT will result in cyber threat information being provided to the organizations best suited to analyze and, to the extent necessary, timely inform responsible entities of cyber threats. In addition, reporting directly to E-ISAC and ICS-CERT addresses the concerns discussed above regarding the confidentiality of reported Cyber Security Incident information. We also find that it is reasonable for NERC to file annually an anonymized report providing an aggregated summary of the reported information, similar to the ICS-CERT annual report. The annual report will provide the Commission, NERC, and the public a better understanding of any Cyber Security Incidents that occurred during the prior year without releasing information on specific responsible entities or Cyber Security Events.

91. Therefore, we conclude that the minimum set of attributes to be reported should 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 or as a result of the Cyber Security Incident. NERC may augment the list should it determine that additional information would benefit situational awareness of cyber threats. As discussed above, we also conclude that NERC should

[144] The DHS ICS-CERT is undergoing a reorganization and rebranding effort. In the event that ICS-CERT no longer exists, its successor will assume the role as incident report recipient.

establish a reporting timeline that provides for notice based upon the severity of the event and the risk to BES reliability, with updates to follow initial reports. We also support the adoption of an online reporting tool to streamline reporting and reduce burdens on responsible entities to the extent the option is available.[145]

E. Other Issues

1. Comments

92. NYPSC supports the NOPR proposal, but notes that if the Commission adopts the NOPR proposal, "the only additional information that state entities would gain is an annual compilation of incidents reported to federal entities."[146] NYPSC claims that an annual report would not provide states with sufficient information on a timely basis so that they can ensure that corrective actions can be taken. Therefore, NYPSC argues that appropriate state entities should also be provided with the cyber reporting information when it is filed with the "federal authorities."

93. Microsoft raises a concern that the NOPR proposal is not clear as to whether the modified CIP Reliability Standards would apply to responsible entities that use a commercial cloud service to operate cloud-based BES Cyber Systems. Specifically, Microsoft requests that the Commission "confirm that cloud service providers that

[145] An online reporting tool will streamline the effort and allow for direct input into a database for a faster turnaround to those that may need to know about the information. For example, *see* https://www.us-cert.gov/forms/report.

[146] NYPSC Comments at 4-5.

provide services to Registered Entities are not required to register with NERC based on their provision of [cloud-based] services, and … are not responsible for compliance with the CIP Reliability Standards."[147] Microsoft asserts that clarifying the status of cloud service providers is important to foster technical innovation.

2. Commission Determination

94. While we appreciate NYPSC's interest in receiving Cyber Security Incident reports when reported to E-ISAC and ICS-CERT, state entities will have access to the same information that is reported to the Commission (i.e., the annual, anonymized summary). Should a state entity determine that it requires additional information from a responsible entity under its jurisdiction, the state entity can work within its own jurisdiction to procure additional information. Our directive is intended to enhance the quality of information received by E-ISAC and ICS-CERT, and directing additional sharing with state entities is outside the scope of this proceeding.

95. We decline to grant Microsoft's requested clarification regarding the potential registration status of cloud service providers because it is outside the scope of this proceeding. Specifically, Microsoft's requested clarification addresses a question regarding registration of cloud service providers under the NERC functional model, as opposed to the specifics of enhanced Cyber Security Incident reporting. The purpose of this proceeding is not to make a determination regarding the registration status of cloud service providers and we have not received input from other interested entities.

[147] Microsoft Comments at 1.

III. Information Collection Statement

96. The FERC-725 information collection requirements contained in this Final Rule are subject to review by the Office of Management and Budget (OMB) under section 3507(d) of the Paperwork Reduction Act of 1995.[148] OMB's regulations require approval of certain information collection requirements imposed by agency rules.[149] Upon approval of a collection of information, OMB will assign an OMB control number and expiration date. Respondents subject to the filing requirements of this 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. The Commission solicits comments on the Commission's need for this information, whether the information will have practical utility, the accuracy of the burden estimates, ways to enhance the quality, utility, and clarity of the information to be collected or retained, and any suggested methods for minimizing respondents' burden, including the use of automated information techniques.

97. The Commission will submit these proposed reporting requirements to OMB for its review and approval under section 3507(d) of the PRA because the Final Rule results in nonsubstantive/non-material changes in paperwork burden. The Final Rule directs NERC to make Cyber Security reporting changes across all applicable Reliability Standards. These proposed changes will be covered by the FERC-725 information collection (Certification of Electric Reliability Organization; Procedures for Electric

[148] 44 U.S.C. 3507(d) (2012).

[149] 5 CFR 1320.11 (2017).

Reliability Standards) [OMB Control No. 1902-0225]). FERC-725 includes the ERO's overall responsibility for developing Reliability Standards to include any Reliability Standards that relate to Cyber Security Incident reporting. There will be no change to the Public Reporting Burden as it affects the FERC-725 information collection.

98. 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.

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

100. Interested persons may obtain information on the reporting requirements by contacting the following: 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].

101. For submitting comments concerning the collection(s) of information and the associated burden estimate(s), please send your comments to the Commission, and to the Office of Management and Budget, Office of Information and Regulatory Affairs, 725 17th Street, NW, Washington, DC 20503 [Attention: Desk Officer for the Federal Energy Regulatory Commission, phone: (202) 395-8528, fax: (202) 395-7285]. For security reasons, comments to OMB should be submitted by e-mail to:

oira_submission@omb.eop.gov. Comments submitted to OMB should include Docket Number RM18-2-000 and OMB Control Number 1902-0225.

IV. Regulatory Flexibility Act Analysis

102. The Regulatory Flexibility Act of 1980 (RFA)[150] generally requires a description and analysis of final rules that will have significant economic impact on a substantial number of small entities.

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

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

V. Environmental Analysis

105. 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.[151] The Commission has categorically excluded certain

[150] 5 U.S.C. 601-612.

[151] *Regulations Implementing the National Environmental Policy Act of 1969*, Order No. 486, FERC Stats. & Regs. ¶ 30,783 (1987).

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.[152] The actions proposed herein to augment current reporting requirements fall within this categorical exclusion in the Commission's regulations.

VI. Document Availability

106. 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.

107. 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. 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

[152] 18 CFR 380.4(a)(2)(ii) (2017).

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.

VII. Effective Date and Congressional Notification

108. The Final Rule is effective [**INSERT DATE 60 days from publication in FEDERAL REGISTER**]. The Commission has determined that this Final Rule imposes no substantial effect upon either NERC or NERC registered entities[153] and, with the concurrence of the Administrator of the Office of Information and Regulatory Affairs of OMB, that this rule is not a "major rule" as defined in section 351 of the Small Business Regulatory Enforcement Fairness Act of 1996. This Final Rule is being submitted to the Senate, House, and Government Accountability Office.

By the Commission.

(S E A L)

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[153] 5 U.S.C 804(3)c

Appendix
Commenters

Jonathan Appelbaum (Appelbaum)
American Public Power Association, Electricity Consumers Resource Council, and Transmission Access Policy Study Group (Trade Associations)
Applied Control Solutions (ACS)
Arizona Public Service Company (APS)
Bonneville Power Administration (BPA)
Edison Electric Institute and National Rural Electric Cooperative Association (EEI/NRECA)
Douglas E. Ellsworth (Ellsworth)
Energy Sector Security Consortium (EnergySec)
Eversource Energy Service Company (Eversource)
Foundation for Resilient Societies (Resilient Societies)
Frank Gaffney (Gaffney)
Idaho Power Company (Idaho Power)
International Transmission Company (ITC)
ISO/RTO Council (IRC)
Isologic LLC (Isologic)
Jerry Ladd (Ladd)
Large Public Power Council (LPPC)
Mary D. Lasky (Lasky)
Michael Mabee (Mabee)
Garland T. McCoy (McCoy)
Microsoft Corporation (Microsoft)
New York Public Service Commission (NYPSC)
North American Electric Reliability Corporation (NERC)
NRG Energy (NRG)
Fred Reitman (Reitman)
Preston L. Schleinkofer (Schleinkofer)
Mark S. Simon (Simon)
Karen Testerman (Testerman)
U.S. Chamber of Commerce (Chamber)