BILLING CODE 6717-01-P
DEPARTMENT OF ENERGY
Federal Energy Regulatory Commission
[Docket No. RD19-3-000]

Petition of North American Electric Reliability Corporation (NERC) for approval of proposed Reliability Standard CIP-008-6 - Cyber Security – Incident Reporting and Response Planning

In Reply Refer To:
North American Electric Reliability
Corporation
Docket No. RD19-3-000

North American Electric Reliability Corporation
1325 G Street, NW
Suite 600
Washington, DC 20005

Attention: Lauren Perotti
Marisa Hecht

Dear Ms. Perotti and Ms. Hecht:

1. On March 7, 2019, the North American Electric Reliability Corporation (NERC) filed a petition requesting approval of proposed Reliability Standard CIP-008-6 (Cyber Security – Incident Reporting and Response Planning). NERC also requested approval of: (1) the associated implementation plan, violation risk factors and violation severity levels; (2) the inclusion of proposed revised definitions of "Cyber Security Incident" and "Reportable Cyber Security Incident" into the NERC Glossary;[1] and (3) the retirement of currently-effective Reliability Standard CIP-008-5. For the reasons discussed below, we grant the requested approvals.

[1] Glossary of Terms Used in NERC Reliability Standards (NERC Glossary).

2. In Order No. 848, the Commission directed NERC to enhance the mandatory reporting of Cyber Security Incidents.[2] The Commission explained that the currently-effective reporting threshold, which only requires reporting in cases where a Cyber Security Incident has "compromised or disrupted one or more reliability tasks," may understate the true scope of cyber-related threats to the Bulk-Power System.[3] To address this reliability gap, pursuant to section 215(d)(5) of the Federal Power Act (FPA), the Commission directed NERC to develop and submit modifications to the Reliability Standard to require the reporting of Cyber Security Incidents that compromise, or attempt to compromise, a responsible entity's Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).[4] With respect to EACMS, the Commission directed that enhanced reporting should apply, at a minimum, to EACMS that perform the following functions: (1) authentication; (2) monitoring and logging; (3) access control; (4) Interactive Remote Access; and (5) alerting.

3. The Commission also directed that 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.[5] The Commission further directed that filing deadlines for Cyber Security Incident reports should be established and that Cyber Security Incident reports should be sent to the Electricity Information Sharing and Analysis Center (E-ISAC) and the Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) or any successor organization.

4. In its petition, NERC states that proposed Reliability Standard CIP-008-6 broadens the mandatory reporting of Cyber Security Incidents and thus addresses the concern that currently-effective Reliability Standard CIP-008-5 may not encompass the full scope of cyber-related threats to the Bulk-Power System.[6] As a predicate to the

---

[2] *Cyber Security Incident Reporting Reliability Standards*, Order No. 848, 164 FERC ¶ 61,033 (2018).

[3] *Id.* PP 2-3.

[4] 16 U.S.C. 824o(d)(5) (2012).

[5] The Commission identified the following minimum fields of information to be reported: "(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." Order No. 848, 164 FERC ¶ 61,033 at P 91.

[6] NERC Petition at 3.

augmented reporting requirements in proposed Reliability Standard CIP-008-6, NERC proposes revised NERC Glossary definitions of Cyber Security Incident and Reportable Cyber Security Incident. NERC explains that, by applying the revised definitions, Cyber Security Incidents (i.e., attempts to compromise) and Reportable Cyber Security Incidents (i.e., actual compromises) will be reported under proposed Reliability Standard CIP-008-6.

5. As proposed by NERC, the revised Cyber Security Incident definition includes events involving "compromises or attempts to compromise" ESPs, EACMS, and Physical Security Perimeters (PSPs) associated with high and medium impact BES Cyber Systems and "disrupt[ion] or attempts to disrupt the operation of a BES Cyber System."[7] NERC contends that the proposed definition of Cyber Security Incident addresses the directives in Order No. 848 because, as discussed below, once a responsible entity determines that an event is a Cyber Security Incident, it must comply with the requirements of proposed Reliability Standard CIP-008-6, including initiating its response plan and reporting the incident to the E-ISAC and, if subject to the jurisdiction of the United States, the National Cybersecurity and Communications Integration Center (NCCIC), which is the successor to ICS-CERT.

6. NERC's proposed revisions to the Reportable Cyber Security Incident definition broaden the scope of reportable events to include compromises or disruptions of BES Cyber Systems that perform one or more reliability tasks as well as compromises or disruptions to EACMS and ESPs associated with high and medium impact BES Cyber Systems. NERC explains that responsible entities will be required to report on a compromise of a BES Cyber System even if it has not affected performance of that BES Cyber System's tasks.[8] For example, NERC states that the revised definition would require responsible entities to report on malware installed on a BES Cyber Asset component of a BES Cyber System that performs one or more reliability tasks regardless of whether the BES Cyber System still operates. NERC indicates that while the revised Reportable Cyber Security Incident definition does not encompass attempts to compromise, under proposed Reliability Standard CIP-008-6, attempts to compromise are reported using the Cyber Security Incident definition.

7. NERC states that proposed Reliability Standard CIP-008-6, Requirement R1, Parts 1.2.1 and 1.2.2 address the Order No. 848 directive to broaden reporting on Cyber

---

[7] NERC indicates that the standard drafting team included all EACMS within the proposed Cyber Security Incident and Reportable Cyber Security incident definitions because nearly all EACMS associated with high and medium impact BES Cyber Systems perform one of the functions identified in Order No. 848. *Id.* at 13-14.

[8] *Id.* at 15.

Security Incidents to include those that "attempt to compromise" an ESP or EACMS.[9] In proposed Requirement R1, Part 1.2.1, each responsible entity must develop a process that includes criteria to evaluate and define attempts to compromise applicable systems. Proposed Requirement R1, Part 1.2.2 requires that each responsible entity develop a process that identifies whether a Cyber Security Incident is an "attempt to compromise" pursuant to the criteria required by Part 1.2.1. NERC explains that Parts 1.2.1 and 1.2.2 work together to help ensure each responsible entity first develops criteria for identifying an attempt to compromise and then applies the criteria during its Cyber Security Incident identification process.[10] NERC maintains that proposed Parts 1.2.1 and 1.2.2 acknowledge the differences in system architecture among responsible entities and provide each responsible entity with the flexibility to develop criteria that reflect what it considers "suspicious." NERC contends that the benefit of such an approach, compared to a one-size-fits-all approach, is that it enables responsible entities to better capture real attempts to compromise.[11]

8. Similar to the proposed revisions in Requirement R1, NERC states that the proposed revisions to Reliability Standard CIP-008-6, Requirement R2 address the Commission's directive in Order No. 848 regarding attempts to compromise.[12] The proposed revisions to Part 2.2 do so by requiring that responsible entities use their Cyber Security Incident response plans when responding to a Cyber Security Incident determined to be an attempt to compromise applicable systems.

NERC contends that proposed Reliability Standard CIP-008-6, Requirement R4 addresses the Commission's directive to require that responsible entities must send each report and update to the E-ISAC and ICS-CERT.[13] Under proposed Reliability Standard CIP-008-6, Requirement R4, Part 4.1, responsible entities are required to submit incident reports for both Reportable Cyber Security Incidents and Cyber Security Incidents. In addition, proposed Reliability Standard CIP-008-6 specifies that the report must contain: (1) the functional impact; (2) the attack vector used; and (3) the achieved or attempted level of intrusion. Proposed Reliability Standard CIP-008-6, Requirement R4, Parts 4.2 and 4.3 include timelines for initial reports as well as follow up reports to the E-ISAC

---

[9] *Id*. at 18.

[10] *Id*.

[11] *Id*. at 19.

[12] *Id*. at 20.

[13] *Id*. at 22.

and NCCIC. NERC states that initial reports for Reportable Cyber Security Incidents must occur within one hour of its determination. By contrast, NERC indicates that once a responsible entity has determined that a Cyber Security Incident meets its criteria for an attempt to compromise an applicable system, it must report the Cyber Security Incident by the end of the next calendar day. NERC justifies the difference by explaining that the "proposed notification timelines appropriately reflect the severity of the risk of the respective incidents."[14] Finally, if a responsible entity does not include one or more of the attributes in its initial report because it was unknown at the time of the initial reporting, it must report the attributes within seven days of determining the attribute.

9. Notice of NERC's March 7, 2019 filing was published in the *Federal Register*, 84 FR 10,061 (2019), with interventions and protests due on or before April 11, 2019. Pursuant to Rule 214 of the Commission's Rules of Practice and Procedure, 18 CFR 385.214 (2018), the timely, unopposed motions to intervene serve to make the entities that filed them parties to this proceeding.[15]

10. Pursuant to section 215(d)(2) of the FPA, we approve Reliability Standard CIP-008-6, its associated implementation plan, violation risk factors and violation severity levels, and the revised definitions of Cyber Security Incident and Reportable Cyber Security Incident.[16] We determine that the proposed Reliability Standard and revised definitions satisfy the directive in Order No. 848 to broaden mandatory reporting to include 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.

Information Collection Statement

11. In compliance with the requirements of the Paperwork Reduction Act of 1995, 44 USC 3506(c)(2)(A), the Commission is soliciting public comment on revisions to the information collection FERC-725B (Mandatory Reliability Standards for Critical

[14] *Id*. at 23.

[15] On April 11, 2019, Public Citizen submitted comments requesting that the Commission direct NERC to require the mandatory public disclosure of entity names in Notices of Penalty for violations of Critical Infrastructure Protection Reliability Standards. Public Citizen's comments do not address proposed Reliability Standard CIP-006-8 or any other proposal contained in NERC's petition, and they are therefore outside the scope of this proceeding.

[16] 16 U.S.C. 824o(d)(2).

Infrastructure Protection (CIP) Reliability Standards), which will be submitted to the Office of Management and Budget (OMB) for a review of the information collection requirements. Comments on the collection of information are due within 60 days of the date this order is published in the *Federal Register*. Respondents subject to the filing requirements of this order will not be penalized for failing to respond to these collections of information unless the collections of information display a valid OMB control number.

12. Proposed Reliability Standard CIP-008-6 requires Responsible Entities[17] to broaden the mandatory reporting of Cyber Security Incidents to include compromises or attempts to compromise BES Cyber Systems or their associated ESPs or EACMS. The revised Reliability Standard will not significantly increase the reporting burden on entities because it builds off the currently-effective reporting threshold by expanding it to address reliability gaps, pursuant to section 215(d)(5) of the FPA.

13. Burden[18] Estimate: The Commission estimates the changes in the annual public reporting burden and cost as indicated below.[19]

RD19-3-000 Commission Letter Order (Mandatory Reliability Standards for Critical Infrastructure Protection Reliability Standards)

[17] "Responsible Entities" refers to Balancing Authority (BA), Distribution Provider (DP), Generator Operator (GOP), Generator Owner (GO), Reliability Coordinator (RC), Transmission Operator (TOP), and Transmission Owner (TO).

[18] Burden is defined as the total time, effort, or financial resources expended by persons to generate, maintain, retain, or disclose or provide information to or for a Federal agency. For further explanation of what is included in the information collection burden, refer to 5 CFR 1320.3.

[19] For the Reliability Standard being retired in Docket No. RD19-3-000, the baseline numbers for respondents, burden, and cost are the same figures as those in Order No. 848. The requirements and burdens (from the Reliability Standard being retired) are continuing in Reliability Standard CIP-008-6, plus the additional requirements and burdens as indicated in the table.

	Number of Respondents & Type of Entity[20] (1)	Annual Number of Responses per Respondent (2)	Total Number of Responses (1)*(2)=(3)	Average Burden & Cost Per Response[21] (4)	Total Annual Burden Hours & Total Annual Cost (3)*(4)=(5)	Cost per Respondent ($) (5)÷(1)
Update internal procedures to comply with augmented reporting requirements. (one-time)[22] (CIP-008-6 R1-R4)	288	1	288	50 hrs.; $4,050	14,400 hrs.; $1,166,400	$4,050
Annual cyber security incident plan review (ongoing)[23] (CIP-008-6 R2.1)	288	1	288	10 hrs.; $810	2880 hrs.; $233,280	$810

[20] There are 1,414 unique registered entities in the NERC compliance registry as of May 24, 2019. Of this total, we estimate that 288 entities will face an increased paperwork burden.

[21] The loaded hourly wage figure (includes benefits) is based on the average of the occupational categories for 2017 found on the Bureau of Labor Statistics website: https://www.bls.gov/oes/2017/may/oessrci.htm.

Legal (Occupation Code: 23-0000): $143.68
Information Security Analysts (Occupation Code 15-1122): $61.55
Computer and Information Systems Managers (Occupation Code: 11-3021): $96.51
Management (Occupation Code: 11-0000): $94.28
Electrical Engineer (Occupation Code: 17-2071): $66.90
Management Analyst (Code: 43-0000): $63.32

These various occupational categories are weighted as follows: [($94.28)(.10) + ($61.55)(.315) + ($66.90)(.02) + ($143.68)(.15) + ($96.51)(.10) + ($63.32)(.315)] = $81.30. The figure is rounded to $81.00 for use in calculating wage figures in this order.

[22] One-time burdens apply in Year 1 only.

[23] Ongoing burdens apply in Year 2 and beyond.

Update cyber security incident plan per review findings (ongoing) (CIP-008-6 R3)	288	1	288	10 hrs.; $810	2880 hrs.; $233,280	$810
Incident reporting burden (ongoing) (CIP-008-6 R4)	288	12	3456	12 hrs.; $972	3456 hrs.; $279,936	$972
TOTAL (one-time)			**288**		**14,400 hrs.; $1,166,400**	
TOTAL (ongoing)			**4032**		**9,216 hrs.; $746,496**	

Title: FERC-725B, Mandatory Reliability Standards for Critical Infrastructure Protection (CIP) Reliability Standards.

Action: Proposed revision to FERC-725B information collection.

OMB Control No: 1902-0248.

Respondents: Responsible Entities.

Frequency of Responses: On occasion.

14. Necessity of the Information: This order approves the requested modifications to Reliability Standards pertaining to critical infrastructure protection. As discussed above, the Commission approves Reliability Standard CIP-008-6 pursuant to section 215(d)(2) of the FPA because it improves upon the currently-effective suite of CIP Reliability Standards.

15. 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.

16. Comments (identified by Docket No. RD19-3-000) concerning the collection of information and the associated burden estimate(s) may also be sent by either of the following methods: eFiling at Commission's Web Site: http://www.ferc.gov/docs-filing/efiling.asp or Mail/Hand Delivery/Courier: Federal Energy Regulatory Commission, Secretary of the Commission, 888 First Street, NE, Washington, DC 20426. Please refer to FERC-725B, OMB Control No. 1902-0248 in your submission.

17. All submissions must be formatted and filed in accordance with submission guidelines at: http://www.ferc.gov/help/submission-guide.asp. For user assistance,

contact FERC Online Support by e-mail at ferconlinesupport@ferc.gov, or by phone at: (866) 208-3676 (toll-free), or (202) 502-8659 for TTY.

By direction of the Commission.

Dated: June 20, 2019.

Nathaniel J. Davis, Sr.,
Deputy Secretary.

[FR Doc. 2019-13587 Filed: 6/25/2019 8:45 am; Publication Date: 6/26/2019]