UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION IN RESPONSE TO NOTICE OF PROPOSED RULEMAKING

The North American Electric Reliability Corporation ("NERC") hereby provides comments on the Federal Energy Regulatory Commission ("Commission") Notice of Proposed Rulemaking ("NOPR") proposing to direct NERC to revise the Critical Infrastructure Protection ("CIP") Reliability Standards to broaden the reporting requirements for Cyber Security Incidents.[1] The NOPR proposes to direct NERC to expand the scope of mandatory reporting to include Cyber Security Incidents that compromise, or attempt to compromise, a Responsible Entity's[2] Electronic Security Perimeter ("ESP") or associated Electronic Access Control or Monitoring Systems ("EACMS").[3] Under the currently effective CIP Reliability Standards, Responsible Entities must report a Cyber Security Incident only if it has "compromised or disrupted one or more reliability tasks of a functional entity."[4]

The Commission also proposes that NERC modify the CIP Reliability Standards to specify minimum required information in Cyber Security Incident reports and establish a deadline for

---

[1] Notice of Proposed Rulemaking, *Cyber Security Incident Reporting Reliability Standards*, 161 FERC ¶ 61,291, Docket Nos. RM18-2-000 and AD17-9-000 (2017) ("NOPR").

[2] The CIP Reliability Standards refer to the Functional Entities to which the standards apply as "Responsible Entities." Responsible Entities include Balancing Authorities, Reliability Coordinators, Transmission Owners, Transmission Operators, Generation Owners, Generation Operators, and certain Distribution Providers.

[3] Unless otherwise designated, all capitalized terms shall have the meaning set forth in the *Glossary of Terms Used in NERC Reliability Standards*, http://www.nerc.com/files/Glossary_of_Terms.pdf.

[4] The *Glossary of Terms Used in NERC Reliability Standards* 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."

filing such reports. The Commission proposes to continue having the reports go to NERC's Electricity Information Sharing and Analysis Center ("E-ISAC") but also require that Responsible Entities send the reports to the Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"). The Commission also proposes to direct NERC to provide the Commission an annual, anonymized summary of the reports received.

In the NOPR, the Commission requests comment on its proposal, including: (1) whether to exclude EACMS from any Commission directive, and instead, establish the compromise, or attempt to compromise, an ESP as the minimum reporting threshold; and (2) whether alternatives to mandatory reporting requirements in a Reliability Standard, such as through a NERC Rules of Procedure ("ROP")[5] Section 1600 data request, would effectively satisfy the goals of the proposed directive.

As described further below, consistent with its recommendation in the 2017 State of Reliability Report,[6] NERC supports broadened reporting of Cyber Security Incidents to allow it to obtain and share additional information to improve the security and reliability of the Bulk Electric System ("BES"). NERC, working with stakeholders, has several initiatives underway to (i) collect cyber security data, (ii) improve cyber security information sharing across the electric sector, and (iii) develop security metrics to help measure BES security. Reporting on incidents that compromise or attempt to compromise an entity's ESP or EACMS would increase awareness and understanding of the scope of cyber-related threats facing the BES and better prepare entities to protect their critical infrastructure from cyber security threats and vulnerabilities.

[5] The NERC Rules of Procedure are located at http://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/NERC_ROP_Effective_20161031.pdf.

[6] The State of Reliability Report 2017 is located at http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/SOR_2017_MASTER_20170613.pdf.

The challenge is to scope any additional mandatory reporting requirement in a manner that collects meaningful data about security risks without creating an unduly burdensome reporting requirement. To that end, NERC supports the Commission's proposal to limit the reporting obligation to Cyber Security Incidents that compromise, or attempt to compromise, a Responsible Entity's ESP or associated EACMS. It is important, however, to precisely outline the parameters of an "attempt to compromise" to ensure that only suspicious activity is reported. Additionally, as the term EACMS covers a wide array of devices that perform different control or monitoring functions, the various types of EACMS present different risks to BES security. As such, it may be necessary to differentiate between the types of EACMS to ensure that any reporting requirement is scoped properly. NERC thus respectfully requests that the Commission provide NERC the flexibility to define "attempts to compromise" and differentiate among EACMS, as necessary, to ensure that any reporting obligation is designed to gather meaningful data without overburdening entities.

Further, NERC requests that the Commission not direct NERC to develop modifications to the Reliability Standards. Instead, the Commission should provide NERC the flexibility to collect the data through alternative approaches, such as the data request process in Section 1600 of the ROP. ROP Section 1600 provides an efficient, mandatory means through which to collect data. In general, NERC is increasing its use of the ROP Section 1600 process to collect data used for system performance[7] rather than collecting the data through Reliability Standards, which typically are more appropriate for data shared between entities for reliable operation of the BES or as evidence of compliance. For example, NERC uses the ROP Section 1600 process to collect quarterly data on Protection System Misoperations.

[7] NERC uses the ROP Section 1600 process to collect system performance information on Demand Response, generator and Transmission availability, and Protection System Misoperations, among others.

These comments are organized into the following sections: Section I.A provides NERC's comments on the scope of the Commission's proposal; Section I.B details NERC's proposed alternative approach to gathering the data through the ROP Section 1600 process; and Section I.C provides NERC's comments on the Commission's proposal regarding the timing and content of entity reports, as well as the proposal to direct NERC to file an annual, anonymized summary of the reports with the Commission.

I. COMMENTS

A. Scope of Commission Directive

1. NERC supports additional reporting of Cyber Security Incidents to increase awareness of cyber security risks to the BES.

NERC appreciates the Commission's concern regarding the reporting of Cyber Security Incidents. Broadening the mandatory reporting of Cyber Security Incidents would help enhance awareness of cyber security risks facing entities. The broadened mandatory reporting would create a more extensive baseline understanding of the nature of cyber security threats and vulnerabilities. This baseline understanding, coupled with the additional context from voluntary reports received by the E-ISAC, would allow NERC and the E-ISAC to share that information broadly throughout the electric industry to better prepare entities to protect their critical infrastructure.

As mentioned previously, broadening reporting of Cyber Security Incidents is consistent with recommendations in NERC's 2017 State of Reliability Report. In that report, NERC noted that cyber security risk extends beyond Reportable Cyber Security Incidents,[8] which include only those Cyber Security Incidents that have "compromised or disrupted one or more reliability tasks of a functional entity."[9] Recognizing that there may be additional risks that could be reported,

[8] The State of Reliability Report 2017 at p. 4.

[9] *Glossary of Terms Used in NERC Reliability Standards* definition of "Reportable Cyber Security Incident."

NERC recommended that NERC and industry "redefine reportable incidents to be more granular and include zero-consequence incidents that might be precursors to something more serious."[10]

To that end, NERC has a number of current efforts underway to facilitate cyber security information sharing. As outlined in its response to the Foundation for Resilient Societies petition for rulemaking in the above-captioned docket AD17-9-000,[11] NERC engages in the following information sharing activities:

- E-ISAC provides its members private-level situational awareness on security threats, physical and cyber security bulletins, access to malware reverse engineering services, remediation, and other security resources.
- E-ISAC facilitates voluntary sharing of information pertaining to physical and cyber threats, vulnerabilities, incidents, and potential protective measures, among others.
- E-ISAC offers malware identification and shares this information with its members.
- E-ISAC conducts outreach events to keep industry informed and prepared for cyber security threats.
- E-ISAC leads security exercises every two years, known as GridEx, which simulate widespread, coordinated cyber and physical attacks on critical electric infrastructure.
- NERC hosts the annual Grid Security Conference where cyber security and physical security experts from industry and government convene to share emerging security trends, policy advancements, and lessons learned related to the electricity sector.
- NERC issues NERC Alerts to provide security information to the electricity industry.
- NERC works with industry stakeholders on the Critical Infrastructure Protection Committee ("CIPC") to discuss relevant cyber and physical security matters and issue guidance documents to address cyber and physical security issues.

[10] The State of Reliability Report 2017 at p. 4.

[11] *Comments of the North American Electric Reliability Corporation in Opposition to Petition for Rulemaking*, Docket No. AD17-9-000 (filed Feb. 17, 2017); *Petition for Rulemaking to Require an Enhanced Reliability Standard to Detect, Report, Mitigate, and Remove Malware from the Bulk-Power System*, Docket No. AD17-9-000 (filed Jan. 13, 2017) (refiled Jan. 19, 2017 with new docket caption).

- NERC and the Regional Entities provide continual outreach to industry to share best security practices at events, such as the Emerging Technology Roundtables.

Since NERC filed its response to the Foundation for Resilient Societies petition for rulemaking, NERC, the Regional Entities, and industry have continued to work together to enhance information sharing on cyber security risks. Among other things, NERC is collaborating with the CIPC Security Metrics Working Group ("SMWG") to develop cyber security metrics using data from various sources to measure cyber security risk. During development of these metrics, NERC and the SMWG have discussed the type of data the Electric Reliability Organization Enterprise ("ERO Enterprise") will need to measure cyber security risk and industry's response to these risks. In addition, the ERO Enterprise has been contemplating the means through which to obtain this data, including through Section 1600 of the ROP. These discussions provide additional context to the metrics included in the ERO Enterprise Strategic Plan and Metrics 2017-2020 that guides the operations of NERC and the Regional Entities.[12] The Commission's NOPR to broaden reporting on Cyber Security Incidents is consistent with these discussions.

2. NERC supports the Commission's proposal to limit the reporting obligation to Cyber Security Incidents that compromise, or attempt to compromise, a Responsible Entity's ESP or associated EACMS.

While NERC supports the Commission's proposal to broaden reporting requirements, those requirements need to be scoped in a manner that provides for meaningful reporting of cyber security risk but does not unduly burden entities. Generating reports on Cyber Security Incidents requires certain resources and capabilities. For example, entities must have the log management infrastructure, log management policies, and staff resources to analyze the data to include in the

[12] The ERO Enterprise Strategic Plan and Metrics 2017-2020 is available at http://www.nerc.com/AboutNERC/StrategicDocuments/ERO_Enterprise_Strategic_Plan_and_Metrics_2017-2020_Clean.pdf.

report. The more data an entity must log, manage, and analyze, the more resources an entity must dedicate to handling that data. If an entity cannot dedicate the appropriate resources to this activity, the data becomes less meaningful because entities cannot process it properly. Therefore, NERC supports scoping the request appropriately to make the burden on entities manageable, resulting in more meaningful data.

NERC thus supports the Commission's proposal to limit the scope of reporting on Cyber Security Incidents to those that compromise, or attempt to compromise, a Responsible Entity's ESP or EACMS. The ESP is the logical border that surrounds those Cyber Assets most important to the BES. The ESP "provides a first layer of defense for network based attacks as it limits reconnaissance of targets, restricts and prohibits traffic to a specified rule set, and assists in containing any successful attacks."[13] EACMS include Cyber Assets that perform electronic access control or monitoring of the ESP or BES Cyber Systems. EACMS encompass a wide variety of devices, such as firewalls, authentication servers, and log monitoring and alerting systems, among others.

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. The ESP and EACMS should not experience a high amount of traffic, unless the entity designed the EACMS to be on an internet gateway. If an entity designed the EACMS to be on an internet gateway, the entity likely implemented a log management infrastructure to address the additional volume of

[13] Reliability Standard CIP-005-5 – Electronic Security Perimeters, Guidelines and Technical Basis at p. 18, http://www.nerc.com/_layouts/PrintStandard.aspx?standardnumber=CIP-005-5&title=Cyber%20Security%20-%20Electronic%20Security%20Perimeter(s)&jurisdiction=United%20States.

data to comply with current CIP Reliability Standards. As a result, the burden on entities may be relatively reasonable, depending on the configuration. Moreover, some EACMS devices in particular may provide important early indicators of future compromise. Therefore, NERC 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. As discussed in the following section, however, given the wide array of EACMS, it may be beneficial to limit the types of EACMS subject to any reporting requirement to scope the requirement appropriately.

Moreover, 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. Pursuant to Reliability Standard CIP-005-5, Responsible Entities must have at least one method, such as an intrusion detection system, for detecting known or suspected malicious communications through medium and high impact Electronic Access Points[14] on ESPs. In addition, Reliability Standard CIP-007-6 requires Responsible Entities to log detected successful and failed login attempts and failed access attempts at the BES Cyber System level or the Cyber Asset level, including EACMS associated with medium and high impact BES Cyber Systems, depending on system or device capability. These types of monitoring and logging activities will assist entities in reporting on attempts to compromise the ESP and EACMS by laying the groundwork for tracking and reporting on such compromises or attempts to compromise.

[14] The *Glossary of Terms Used in NERC Reliability Standards* defines "Electronic Access Points" as "A Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter." The CIP Reliability Standards require bi-directional routable communications to pass through an Electronic Access Point when communicating with Cyber Assets within an ESP.

3. NERC requests flexibility to scope the proposed reporting threshold more precisely to gather meaningful data without overburdening entities.

As discussed above, while NERC is supportive of the general scope proposed by the Commission, NERC recognizes 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. NERC identified at least two items that require additional focus.

First, NERC needs to outline the parameters of an "attempt to compromise" in order to issue a precise data request. Monitoring suspicious activities varies across entities; what may appear to be an "attempt to compromise" for one entity may be a normal activity for another entity. NERC would develop a common threshold for an "attempt to compromise" for reporting purposes, taking into account the variety of suspicious activity. NERC would consider the common understanding of adverse activities that are early indicators of compromise, such as campaigns against industrial control systems, to help define the parameters.

Second, as defined in the NERC Glossary, EACMS include a wide variety of devices that perform control or monitoring functions. The risks posed by these various systems may differ substantially. It is important to focus industry resources on higher risk systems. Certain devices that qualify as EACMS may have no or minimal impact on the security of BES Cyber Systems if compromised. NERC thus needs to consider whether to define the reporting threshold to differentiate between the various types of EACMS for reporting purposes.

For these reasons, NERC respectfully requests that the Commission provide NERC the flexibility to refine the thresholds for reporting, including defining "attempts to compromise" and differentiating between EACMS, as necessary, to ensure that any reporting obligation is designed to gather meaningful data without overburdening entities.

B. NERC requests that the Commission not issue a directive to modify Reliability Standards but allow NERC to use the process in Section 1600 of its ROP for collecting the data.

Although NERC supports broadening Cyber Security Incident reporting, NERC requests that the Commission not direct NERC to modify the CIP Reliability Standards. Instead, the Commission should grant NERC the flexibility to determine the appropriate method through which to obtain the additional data. Specifically, NERC would use the ROP Section 1600 process for data requests to collect the information from industry. As noted above, NERC seeks to use the ROP Section 1600 process instead of Reliability Standards for gathering data used for system performance. NERC has successfully shifted to using Section 1600 for other data collection efforts, such as the collection of reports on Protection System Misoperations. The ROP Section 1600 process would supplement the existing voluntary reporting of cyber security threats to the E-ISAC.

The ROP Section 1600 data request process provides many of the same benefits as Reliability Standards. Similar to Reliability Standards development, the process requires stakeholder and Commission staff input. Section 1602 of the NERC Rules of Procedure dictates that NERC post a proposed data request for a 45-day public comment period. NERC considers stakeholder input from the comment period to improve upon the proposed data request. NERC publicly posts the received comments and, in seeking NERC Board of Trustees authorization to issue the data request, provides an explanation on how NERC addressed stakeholder comments. In addition, FERC staff has the opportunity to review the proposed data request. Under ROP Section 1600, NERC must provide the proposed data request to the Commission's Office of Electric Reliability 21 days prior to the public posting.

Like Reliability Standards, compliance with a ROP Section 1600 data request is mandatory for applicable entities. In the past, entities subject to a ROP Section 1600 data request responded

in a timely and comprehensive manner. In the event entities are not responsive, however, NERC has the authority under the ROP 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.[15] NERC may enforce a data request by submitting a request for enforcement of compliance with ROP Section 1600 data requests to the Commission's enforcement staff.

ROP Section 1600 allows for an efficient process for revising or updating the data request, if such a need arises. The Reliability Standards process requires multiple approvals from the NERC Standards Committee at various points during the project, a two-thirds majority stakeholder approval, NERC Board of Trustees adoption, and, finally, Commission approval. The ROP Section 1600 process is more streamlined, requiring a 21-day Commission review period, a 45-day public comment period, and NERC Board of Trustees authorization. Further, minor revisions to an authorized ROP Section 1600 data request do not need Board of Trustees approval.

While the Reliability Standards process serves as an appropriate check-and-balance in developing high quality, technically accurate Reliability Standards, that process may not be best suited to developing a reporting requirement for cyber security compromises or attempts to compromise. As security threats are constantly evolving, NERC may need to modify the reporting requirement more frequently and on a shorter timeframe than the standards development process may allow. NERC does not intend to revise the request on a regular basis but appreciates the flexibility to modify the reporting requirement provided by the ROP Section 1600 process should the need arise. Additionally, as the balance between obtaining additional data on cyber security risks and the burden it imposes on entities may shift over time, an efficient process for revising

[15] Rules of Procedure of the North American Electric Reliability Corporation, Section 100.

any reporting requirement is important. The streamlined ROP Section 1600 process allows NERC to modify the data request based on its needs to assess cyber security risk.

Because of the advantages discussed above, NERC is moving towards removing data collection for system performance purposes outside of mandatory standards and into ROP Section 1600 data requests. NERC may continue using data collection in Reliability Standards for evidence of compliance or for requiring information sharing between entities for reliable operation of the BES, among other purposes, but has found the ROP Section 1600 process to be effective for data collection to assess system performance. For instance, NERC currently has a standing ROP Section 1600 data request for entities to submit quarterly data on Protection System Misoperations.[16] Among other things, the data request asks for information describing the Protection System failure event, type of equipment involved, and the category of Misoperation as defined by tables in the data request.[17] All U.S. Transmission Owners, Generator Owners, and Distribution Providers on the NERC Compliance Registry must submit data on a per-entity basis. NERC collects the data to inform statistics on Misoperations, identify risks to the BES, and share lessons learned with the electric industry.

The use of ROP Section 1600 is appropriate for collecting data in high priority areas. Similar to NERC's findings on cyber security risk in the 2017 State of Reliability report, the 2012 and 2013 State of Reliability reports identified Protection System Misoperations as one of the top risks to reliability.[18] Based on recommendations in those reports, a task force analyzed the top

---

[16] *Request for Data or Information: Protection System Misoperation Data Collection* (Aug. 14, 2014), http://www.nerc.com/pa/RAPA/ProctectionSystemMisoperations/PRC-004-3%20Section%201600%20Data%20Request_20140729.pdf.

[17] *Id*. at 11.

[18] The 2012 State of Reliability Report is located at http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2012_SOR.pdf and the 2013 State of Reliability Report is located at http://www.nerc.com/pa/RAPA/PA/Performance%20Analysis%20DL/2013_SOR_May%2015.pdf.

three causes of Misoperations as identified by data collected pursuant to Reliability Standard PRC-004-002.1a. As NERC improved upon and streamlined PRC-004 in version 3 of that Reliability Standard, NERC removed the reporting requirement from the Reliability Standard and started collecting Misoperations data through the ROP Section 1600 instead. Entities have been responsive to the data request in providing comprehensive data to NERC. Through this ongoing collection and identification of the top causes of Misoperations using the data, NERC educated industry on actions that could address common causes of Misoperations.

The ROP Section 1600 data request process also provides the flexibility to determine the appropriate timeline for submitting the data. Whereas entities submit quarterly data in response to the Protection System Misoperations data request, NERC may select any appropriate timeframe for submitting the data on Cyber Security Incidents. In the case of the data request for Cyber Security Incident reports, for instance, the ROP Section 1600 process provides NERC the flexibility to request data closer in time to the occurrence of the compromise or attempt to compromise, if this timeframe is necessary. This permits NERC to receive the data as early indicators of compromise. NERC also may elect to request data on a weekly, monthly, or quarterly basis depending on the purpose of the data requested. NERC will determine the appropriate timeline based on an assessment of the risk the data is addressing versus the burden on entities to produce the data in the requested timeframe.

Finally, the ROP Section 1600 complements the existing industry practice of voluntary reporting to the E-ISAC. NERC appreciates the importance of freely sharing information on cyber or physical security threats among industry stakeholders, particularly when such attacks may move quickly. E-ISAC facilitates this practice outside of the ERO Enterprise Compliance Monitoring

and Enforcement Program and the ROP Section 1600 process. The ROP Section 1600 data request will supplement, not replace, the voluntary information sharing already occurring among industry.

C. NERC supports the Commission's proposal on the content, timing, and filing of an annual, anonymized summary of reports.

NERC supports the proposal to impose a deadline on when entities must send full reports of Cyber Security Incidents to NERC, but NERC requests flexibility to determine the appropriate timeframe. The timeliness of the data received will likely impact how it is used. Data on attempts to compromise received within 24 hours to a few days provides an early indication of potential attacks whereas data received monthly factors into analysis of trends in activity over time. NERC 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. These timelines would complement existing reports; Reliability Standard CIP-008-5 requires notifying the E-ISAC of incidents that have an impact within an hour.

NERC also supports the content of reports on Cyber Security Incidents as proposed by the Commission. The Commission proposes each report include the following: (1) the functional impact of the attack or attempted attack, (2) the attack vector, and (3) the level of intrusion. NERC agrees 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. NERC also does not oppose filing an annual, anonymized summary of the reports with the Commission. Finally, NERC also does not oppose the Commission's proposal to submit the reports of U.S.-based entities to the ICS-CERT in addition to the E-ISAC.

II. CONCLUSION

For the reasons stated above, NERC supports the proposed broadening of reporting of Cyber Security Incidents. NERC respectfully requests, however, that the Commission properly limit any proposed directive and consider the above comments to help ensure that any reporting requirement is appropriately scoped. NERC also respectfully requests that the Commission provide NERC the flexibility to consider alternative means of collecting the data outside of mandatory Reliability Standards.

Respectfully submitted,

/s/ Marisa Hecht

Shamai Elstein
Senior Counsel
Marisa Hecht
Counsel
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
shamai.elstein@nerc.net
marisa.hecht@nerc.net

Counsel for the North American Electric Reliability Corporation

Date: February 26, 2018

CERTIFICATE OF SERVICE

I hereby certify that I have served a copy of the foregoing document upon all parties listed on the official service lists compiled by the Secretary in Docket Nos. RM18-2-000 and AD17-9-000.

Dated at Washington, DC this 26th day of February, 2018.

/s/ Marilani Alt

Marilani Alt
Legal Assistant
North American Electric Reliability Corporation
1325 G Street, N.W., Suite 600
Washington, DC 20005
(202) 400-3000
marilani.alt@nerc.net