UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

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

COMMENTS OF THE EDISON ELECTRIC INSTITUTE AND THE NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

I. INTRODUCTION

The Edison Electric Institute ("EEI") and the National Rural Electric Cooperative Association ("NRECA"), on behalf of our member companies, hereby respectfully submit comments in response to the Notice of Proposed Rulemaking ("NOPR") issued by the Federal Energy Regulatory Commission ("the Commission" or "FERC") on December 21, 2017, in the above-referenced docket.[1]

EEI is the association that represents all U.S. investor-owned electric companies. Our members provide electricity for about 220 million Americans, and operate in all 50 states and the District of Columbia. As a whole, the electric power industry supports more than 7 million jobs in communities across the United States. In addition to our U.S. members, EEI has more than 60 international electric companies, with operations in more than 90 countries, as International Members, and hundreds of industry suppliers and related organizations as Associate Members.

[1] *Cyber Security Incident Reporting Reliability Standards*, 161 FERC ¶ 61,291 (2017) ("NOPR").

Organized in 1933, EEI provides public policy leadership, strategic business intelligence, and essential conferences and forums. EEI's U.S. members include Generator Owners and Operators, Transmission Owners and Operators, Load-Serving Entities, and other entities that are subject to the mandatory Reliability Standards developed by the North American Electric Reliability Corporation ("NERC") and enforced by NERC and the Commission.

NRECA represents the interests of the nation's more than 900 rural electric utilities responsible for keeping the lights on for more than 42 million people across 47 states. Electric cooperatives are driven by their purpose to power communities and empower their members to improve their quality of life. Affordable electricity is the lifeblood of the American economy, and for 75 years electric co-ops have been proud to keep the lights on. Because of their critical role in providing affordable, reliable, and universally accessible electric service, electric cooperatives are vital to the economic health of the communities they serve. Additionally, NRECA's members participate in all of the organized wholesale electricity markets throughout the country. And for this reason, NRECA participates in a variety of Commission proceedings, rulemakings and notices of inquiries on behalf of its members affecting the reliability of the BES.

Accordingly, EEI and NRECA members are directly affected by the NOPR. EEI and NRECA agree with and support the Commission in declining to propose additional Reliability Standard modifications to address malware detection, mitigation, and removal because malware is already addressed by existing efforts. However, as discussed herein, we do not support the Commission's Cyber Security Incident reporting modifications as proposed in the NOPR.

II. COMMENTS

The existing Critical Infrastructure Protection ("CIP") Reliability Standards, require responsible entities to implement and maintain processes to notify the Electricity Information Sharing and Analysis Center ("E-ISAC") within one hour from the determination of "a Cyber Security Incident that has compromised or disrupted one or more reliability tasks of a functional entity" ("Reportable Cyber Security Incident").[2] The Department of Energy ("DOE") OE-417 Form also requires responsible entities to submit an initial report on physical attacks and cyber events that "could potentially impact electric power system adequacy or reliability" within six hours of the incident and a final report within 72 hours.[3]

In the NOPR, the Commission proposes to direct NERC to modify the CIP Reliability Standards to increase the Cyber Security Incident reporting threshold to the E-ISAC, require responsible entities to also report Cyber Security Incidents to the Department of Homeland Security ("DHS") Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT"), specify the required reporting information, mandate reporting timeframes, and require NERC to annually file an anonymized public summary of the reports.[4] The proposed new reporting threshold would add incidents that compromise Electronic Access Control or Monitoring Systems ("EACMS") and attempts to compromise a responsible entity's Electronic Security Perimeter ("ESP") or associated EACMS to the existing threshold.

The Commission proposes these modifications due to concerns that the current reporting

[2] CIP-008-5 – Cyber Security – Incident Reporting and Response Planning, NERC Glossary of Terms.

[3] DOE OE-417 Form

[4] NOPR at P 2, 4.

threshold "may not reflect the true scope of cyber-related threats facing the Bulk-Power System."[5] In the NOPR, FERC identified the low number of Reportable Cyber Security Incidents reported to the E-ISAC in 2014 and 2015 compared to the DHS ICS-CERT reports[6] as a gap in the current mandatory reporting requirements. With these proposed modifications, the Commission seeks to increase the volume of mandatory reporting of Cyber Security Incidents to "improve awareness of existing and future cyber security threats and potential vulnerabilities"[7] for "NERC, industry, the Commission, other federal and state entities, and interested stakeholders."[8]

EEI and NRECA do not support the Commission's NOPR proposals. More work is needed to determine what useful and meaningful information can be collected that is not already addressed by existing voluntary threat information sharing efforts. More work is also needed to address the related challenges and potential unintended consequences created by the Commission's proposed directives. EEI and NRECA encourage the Commission to pursue this work before directing NERC to modify the standards or engage in mandatory information collections.

Although cybersecurity threat and vulnerability awareness is important, responsible entities already closely coordinate with a number of organizations, including the E-ISAC, DOE, DHS, the Federal Bureau of Investigation ("FBI"), the National Laboratories, and vendors to detect, analyze, and share threat and vulnerability information through voluntary partnerships.

[5] *Id*. at P 24.

[6] There were zero Reportable Cyber Security Incidents in 2014 and three in 2015, whereas there were 79 cybersecurity incidents reported to DHS ICS-CERT in 2014 and 46 in 2015. NOPR at P 10.

[7] *Id*. at P 24.

[8] *Id*. at P 4.

EEI and NRECA are also concerned that modifying the CIP Standards to mandate this information sharing would weaken these important voluntary security partnerships. We recommend that the Commission conduct a conference or workshop to carefully consider the challenges and potential unintended consequences discussed below with stakeholders before mandating additional information collection.

A. The proposed modifications raise technical, regulatory, and administrative challenges that may bring unintended consequences.

The Commission proposes modifications to the existing mandatory reporting of Cyber Security Incidents to increase the reporting threshold, content specificity, and number of organizations to which responsible entities must submit reports. Each of these proposed modifications introduces new challenges that should be addressed before directing NERC to mandate further collection of information.

Adding attempted compromises to the existing mandatory CIP-008 reporting requirements will broaden the purpose of this reporting from system restoration to threat intelligence. The existing mandatory incident reporting requirements in CIP-008-5 are focused on notifying the E-ISAC of cybersecurity incidents and disruptions caused by actual compromises to aid in response efforts. Voluntary reporting to DHS ICS-CERT is also focused on incident response and recovery. The Commission should adhere to their conclusion in Order No. 706 that reportable cyber incidents "should not be triggered by ineffectual and untargeted attacks that proliferate on the internet."[9] However, if the Commission is seeking to change its direction, then the reliability need should be better defined and balanced with the challenges and burdens introduced by the new requirements.

[9] Order No. 706 at P 661.

The Commission's intent regarding adding "attempted compromise" to the reporting threshold is unclear. A clear understanding of what an "attempted compromise" means is needed to assess the impact of the proposed modifications because the term is currently undefined and may vary by the ability of responsible entities (and auditors) to identify such attempts. For example, if an entity has an anomaly detection tool, then they may be able to identify unusual or unexpected communication signals to an electronic access control system; however, determining whether this is an attempted compromise would require further analysis to determine whether the signal was a deliberate attempt to compromise the system. However, implementing such tools can be challenging and the analysis needed to determine whether observed activity is an actual attempt to compromise a system is likely to be resource intensive.

Another example of the ambiguity of the Commission's proposal is related to the number of attempted phishing attacks on utilities, one of the attack vectors identified by the Commission.[10] Phishing attacks seek to trick recipients into disclosing information, such as access credentials. An individual with access to medium or high impact Bulk Electric System ("BES") Cyber Systems and/or their associated EACMS devices may receive a phishing email, this could be seen as an "attempted compromise" of the protected assets to which that individual has access. However, given the sophistication of utility email protections and the separation implemented between corporate information systems and BES Cyber Systems, mandated by the CIP Standards, the overwhelming majority of these attacks are automatically stopped at corporate borders and never appear in an individual's inbox. Investigating, analyzing, and reporting each of those phishing attempts, any of which, if successful "might facilitate

[10] NOPR at P 39.

subsequent efforts to harm the reliable operation of the bulk electric system,"[11] would be extremely burdensome given the sheer number of attempts. Without more detail regarding what an attempted compromise means or entails, responsible entities may be required to report all zero consequence incidents. Given the sheer number of incidents this could entail, it is also not clear that this level of reporting would "reflect the true scope and scale of cyber-related threats facing the Bulk-Power System."[12]

Identifying attempted compromises is particularly challenging for EACMS as some of these devices such as firewalls can be on a corporate network that may deny high volumes of traffic that could be considered attempts to compromise. For some companies this can be thousands to millions of "attempts" per day, depending on how an attempt to compromise is defined. Much of these attempts are not likely to be malicious attempts, but entities would have to inspect and analyze every packet that attempts to enter their network to filter through all of the rejected the noise and "find the needle in the haystack" based on a determination of a sender's intent. Also, determining what "might be" a precursor to "something more serious" or "could cause harm" would be very difficult for entities to define and determine, and equally difficult for auditors to sufficiently define and audit. This is the very reason entities are relying on partnerships with government and vendor services to help them identify such traffic through automated tools such as CRISP and CYOTE, which are discussed further below.

Given the variety of technologies being used by and the various analytical capabilities of responsible entities, it is unclear what would be a reasonable expectation for such analysis and

[11] *Id*. at P 24.

[12] *Id*. at P. 24.

reporting. Determining what to monitor and collect can be challenging on OT networks because there are a wide variety of devices with proprietary operating systems and applications that do not have traditional information technology ("IT") logging capabilities. For example, many OT networks are not built to handle the large amounts of data necessary for event logging. Also, significant effort is required for a responsible entity to be able to baseline network communication traffic to include all OT protocols and ensure that all factors (e.g., RTU protocols, storm mode, other BES system disturbances) are accounted for when identifying anomalies. More work needs to be done to determine the technical feasibility, if any, of identifying and analyzing potential attempted compromises before NERC can begin drafting modifications to the CIP standards or issuing data requests. Without additional clarity, there is the potential of over-reporting of benign activity that will not aid reliability and could significantly divert resources and create administrative burdens that may be detrimental to reliability and to those organizations responsible for discerning credible threats versus "noise" in the existing information sharing environment.

In addition to these ambiguities and related technical challenges, there may be regulatory challenges created by the Commission's proposed modifications. For example, the information the Commission is proposing to require responsible entities to submit to the E-ISAC and DHS may be considered BES Cyber System Information, which is an emerging challenge regarding sharing with third parties such as service providers who provide threat analysis services. Creating new regulatory challenges could slow innovation among responsible entities, undermining their ability to improve their reliability and security. For example, responsible entities may increasingly recognize benefits in leveraging technology vendors, such as cloud service providers, for functions that do not directly operate the BES but integrate closely with

such systems and may be considered an extension of the ESP. The Commission's proposed modifications may undermine the ability for responsible entities to leverage new technologies and security innovations if there is not clarity regarding the regulatory impacts.

Security challenges should also be considered by the Commission. The Commission proposes to require responsible entities to report on specific attack attributes, including the functional impact, attack vector, and level of intrusion achieved or attempted by an attacker.[13] Although these attributes could be useful to improve responsible entity awareness of the threat so that they can tailor their defenses to address such threats, reporting such information publicly,[14] would provide attackers useful information on the best methods to impact particular functions and the best ways to attack responsible entities. The resulting unintended consequence is helping attackers, who are more agile than the responsible entities that must defend all of their systems for reliability, security, and compliance.

Redundant and unnecessary reporting is also a concern. Responsible entities are already required to report cybersecurity incidents to DOE under Form OE-417 and to the E-ISAC by CIP-008-5. Adding DHS ICS-CERT as a third recipient of cybersecurity incident reports is not necessary because the E-ISAC already coordinates with DHS through the National Cybersecurity and Communications Integration Center ("NCCIC"), of which DHS ICS-CERT is now a part. Also, additional reporting to DHS is inconsistent with the Paperwork Reduction Act. The purpose of the Paperwork Reduction Act is to minimize the paperwork burden "from the

[13] *Id*. at P 38.

[14] DHS ICS-CERT provides annual, anonymized sector reports of incidents that are made public and the Commission proposes to direct NERC to provide similar, public reports. *Id*. at P 42.

collection of information by or for the Federal Government."[15] In the NOPR, the Commission proposes to direct NERC to modify the Reliability Standards to require responsible entities to report the same information to NERC and DHS, which is essentially a double, redundant collection of information from responsible entities. If approved by the Commission, both NERC and the Commission would enforce this information collection.

Mandating further threat information sharing could also harm the ability or desire of responsible entities to participate in existing voluntary partnerships. Although threat intelligence is aligned with the E-ISAC mission, it is a part of their voluntary mission. New mandatory reporting requirements—especially the challenging requirements proposed by the Commission (e.g., identifying attempted compromises)—would require responsible entities to shift resources from the voluntary threat information sharing partnerships to focus on compliance activities such as documenting evidence of such reporting for audits by NERC and the Commission. If threat information sharing becomes a compliance activity, it may have an unintended consequence of limiting the sharing of incidents to the content required by the standard for some entities. For example, what a responsible entity must do for compliance would be given priority over what it could do to enhance security, especially for entities with more limited threat intelligence resources.

Mandatory reporting is also not within the ICS-CERT mission "to reduce risk to the Nation's critical infrastructure by strengthening the security and resilience of control systems through public-private partnerships."[16] Mandating reporting is contrary to this partnership

[15] Paperwork Reduction Act, purpose.

[16] DHS ICS-CERT website.

mission. There are also key differences between the DHS ICS-CERT reporting and the CIP Standards reporting of Reportable Cyber Security Incidents. The voluntary DHS reporting includes not only electric companies, but also oil and natural gas companies, whereas the CIP Standards reporting is focused on responsible entities in the electricity subsector that are subject to the NERC CIP Standards.[17] The DHS reporting is also focused on all industrial control systems and it is unclear where the boundaries exist as many of the reports are categorized as spear phishing and network scanning, which is activity that is more likely found on IT or corporate networks. Voluntary reporting for OT systems have many of the same challenges discussed above, which also limit the ability for the Energy Sector and other critical infrastructure sectors to report to DHS. Whereas, Reportable Cyber Security Incidents are appropriately focused on actual compromises of the ESP and PSP of medium and high impact BES Cyber Systems to aid in incident response and recovery efforts. These differences make it difficult to determine whether there is an actual reliability gap that requires mandating new requirements or data requests.

Finally, the absence of Reportable Cyber Security Incidents is not necessarily an indicator of a reliability gap. However, such an absence in reports is an indicator of reliability since they are tied to actual compromises that may impact reliability tasks. Also, the Commission relies on the Foundation for Resilient Societies assertion that "current mandatory and voluntary cybersecurity incident reporting methodologies are not representative of the actual annual rate of occurrence of cybersecurity incidents" in proposing new reporting requirements. However, a thorough examination is not yet evidenced in the record of the existing voluntary

[17] See NOPR at fn. 41.

cybersecurity incident reporting, including reporting and tracking of incidents by government agencies and vendors.[18]

The Commission should carefully consider these challenges and the impacts its decisions may have on responsible entities and their partnerships with vendors and government such as DHS ICS-CERT, which could have unintended consequences on BES reliability.

B. Existing partnerships are already focused on threat and vulnerability sharing; mandating such information sharing could harm these efforts.

Responsible entities are partnered with a number of organizations, including the E-ISAC, DOE, the FBI, the National Laboratories, DHS, and various product and service providers to share threat and vulnerability information. Through these partnerships, the expertise and innovation of both industry and government is harnessed to improve threat and vulnerability detection, analysis, and sharing capabilities. Significant resources from responsible entities and government are engaged in these partnerships. For example, the E-ISAC, in coordination with and in investment by its members has been maturing into a customer-focused service. The E-ISAC provides a valuable resource to its members as a vehicle for sharing and receiving cyber and physical security threat information. Mandating 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.

Executives and subject matter experts already focus on identifying, sharing, and analyzing threat information such as attempted compromises. Chief Executive Officers ("CEOs") and other responsible entity executives work directly with the E-ISAC, DOE, National

[18] The reporting assertions in the Petition by the Foundation for Resilient Societies were made "on information and belief" rather than actual evidence. Foundation for Resilient Societies, Petition for Rulemaking at 8-9, Docket No. AD17-9 filed Jan 13, 2017.

Laboratories, and DHS. Responsible entity cybersecurity—not compliance—experts share significant amounts of data with the government, including detected unusual or suspicious activity. Government analysts work with responsible entities and the E-ISAC to analyze this data and compare it to known threat indicators to identify potential threats and vulnerabilities. Innovative threat intelligence platforms and technologies have also been developed and deployed under these partnerships.

For example, the Cybersecurity Risk Information Sharing Program (CRISP) leverages advanced sensors deployed on responsible entity systems and threat analysis techniques for bi-directional sharing of classified and unclassified threat information.[19] CRISP is managed by the E-ISAC and is a partnership between DOE, NERC, and electric companies for rapid sharing and analysis of threat information.[20] DOE's National Laboratories support the deployment of the information sharing technologies and infrastructure as well as the technical analysis for CRISP. The network sensors for CRISP are deployed at a responsible entity's network border, just outside the corporate firewall. As a result, network traffic for the entire network or company—not just BES Cyber Systems—is analyzed to detect potential threats and vulnerabilities, which helps electric companies fine tune their firewalls and other cybersecurity technologies and strategies to prevent cybersecurity incidents.

[19] Department of Energy, https://energy.gov/oe/energy-sector-cybersecurity-preparedness-0. RSA Conference Presentation, https://www.rsaconference.com/writable/presentations/file_upload/png-f01_the_cybersecurity_risk_information_sharing_program-final.pdf

[20] Utilities participating in CRISP provide electricity to over 75% of customers in the continental United States. Testimony of Acting Assistant Secretary Patricia Hoffman, Before the Committee on Homeland Security Subcommittee on Cybersecurity and Infrastructure Protection, at 5 (Oct. 3, 2017), located at: http://docs.house.gov/meetings/HM/HM08/20171003/106448/HHRG-115-HM08-Wstate-HoffmanP-20171003.pdf.

DHS has also partnered with Commercial Service Providers through their Enhanced Cybersecurity Services ("ECS") program to share vetted sensitive and classified government cyber threat information, which can supplement existing commercial services and capabilities, which are available to all critical infrastructure sectors.[21] In addition, the DHS Cyber Information Sharing and Collaboration Program ("CISCP") is another example of a multi-directional cybersecurity information sharing and analytic partnership between the government and industry.[22] DHS also has an Automated Indicator Sharing ("AIS") program for automated, machine-to-machine sharing of threat information; however, the threat indicators are not validated by the government and rely on participants to help validate.[23]

Although these efforts primarily focus on the corporate networks, DOE has a pilot project—the Cybersecurity for the Operational Technology Environment ("CYOTE")—that seeks to expand the real-time sharing and analysis provided by programs such as CRISP to the operational technology ("OT") environment.[24] As a part of this pilot, DOE and industry are identifying and addressing challenges related to collecting and sharing data on OT networks, including what to monitor and how to collect, process, and share sensitive data.[25]

Common to these sharing partnerships is the fact that they are voluntary, based on trust, and focused on enhancing critical infrastructure cybersecurity. Mandating such sharing may weaken the ability of electric companies to participate in these programs by shifting their focus

[21] Department of Homeland Security, Enhanced Cybersecurity Services, https://www.dhs.gov/sites/default/files/publications/ECS-Fact-Sheet-0814-508.pdf

[22] Department of Homeland Security, Cyber Information Sharing and Collaboration Program, https://www.dhs.gov/ciscp

[23] Department of Homeland Security, Automated Indicator Sharing, https://www.us-cert.gov/ais.

[24] Department of Energy, https://energy.gov/oe/energy-sector-cybersecurity-preparedness-0

[25] *Id*.

to compliance activity. Reducing electric company participation may also harm these voluntary programs and their ability to enhance critical infrastructure cybersecurity. The Commission should carefully consider the impacts its decisions may have on these partnerships before directing further reporting requirements.

C. The Commission should focus on enhancing existing voluntary partnerships rather than creating redundant mandatory reporting.

Due to the potential impacts on existing, voluntary partnerships focused on threat intelligence and associated technical and administrative challenges discussed above, EEI and NRECA recommend that the Commission continue to limit the focus of CIP-008 to reporting on actual compromises of the ESPs of high and medium impact BES Cyber Systems to the E-ISAC to aid with incident response and restoration. To address the challenges discussed above associated with identification and reporting on attempted compromises, a term that experts can interpret differently, as well as the impacts on partnerships and security of the BES, the Commission should consider methods to further study these challenges and seek to enhance the existing threat intelligence partnerships rather than mandate redundant and potentially burdensome requirements.

EEI and NRECA recommend that rather than issuing a final rule, the Commission should conduct a technical conference or workshop to further explore the need for additional reporting, the definition of "attempted compromise," and the feasibility of reporting attempted compromises for BES Cyber Systems as well as the associated challenges, burdens, and benefits to BES reliability. Before introducing new reporting requirements, the Commission should convene organizations involved in threat sharing, including responsible entities, DOE, DHS, the E-ISAC, and vendors. This group could discuss anticipated impacts of the modifications, the Commission's desired outcomes, and regulated entities' and third parties' capabilities and

current investments that may provide an alternate means of achieving the Commission's desired outcomes. A conference or workshop would provide a forum to discuss the challenges of different stakeholders to reveal potential unintended consequences of the Commission's directives.

Such a forum would also allow for a discussion on the types of incidents that are reasonable for responsible entities to report. For example, participants could evaluate and examine the difference between zero-consequence incidents and, as NERC recommended for reporting, "zero-consequence incidents that might be precursors to something more serious."[26] Also, technical conferences are more likely to engage a broader stakeholder audience such as service providers whose services may be impacted by the Commission's directives and other government agencies such as DOE and DHS, who are all unlikely to participate in the standards development process or comment on NERC's section 1600 data requests.

III. CONCLUSION

EEI and NRECA appreciate the opportunity to submit comments in response to the NOPR. As discussed above, The Commission should limit mandatory reporting to the E-ISAC and to actual compromises of the ESP. We do not support the modifications proposed by the Commission in the NOPR because more work is needed to: clarify what information is needed that is not already addressed through voluntary threat information sharing, better understand the meaning of "attempted compromise," discuss the associated challenges and potential unintended consequences created by the Commission's proposals, avoid creating redundant and unnecessary reporting requirements, and avoid harming existing threat information sharing partnerships. For

[26] NOPR at P. 29.

these reasons, EEI and NRECA recommend that the Commission convene a technical conference or workshop to flesh out these concerns before directing NERC to mandate new Cyber Security Incident information collections.

Respectfully submitted,

EDISON ELECTRIC INSTITUTE

/s/ Scott I. Aaronson
Vice President, Security & Preparedness

Melanie Seader
Associate General Counsel, Reliability and Security
mseader@eei.org

Edison Electric Institute
Washington, D.C. 20004
(202) 508-5000

NATIONAL RURAL ELECTRIC COOPERATIVE ASSOCIATION

/s/ Randolph Elliott
Senior Director, Regulatory Counsel
randolph.elliott@nreca.coop

Barry Lawson
Senior Director, Regulatory Affairs
barry.lawson@nreca.coop

National Rural Electric Cooperative Association
4301 Wilson Boulevard
Arlington, VA 22203
(703) 907-6818

Dated: February 26, 2018

Document Content(s)